EXHIBIT B-3

Chapter 4: The Role of Cylance Inc.

Cylance Inc.'s information security tools detected critical malicious code and other threats to OPM's network in April 2015. While Cylance tools were available to OPM as early as June 2014, OPM did not deploy its preventative technology until after the agency was severely compromised and the nation's most sensitive information was lost. OPM's IT security operations recommended deploying Cylance's preventative technology, CylanceProtect (Protect), to insulate OPM's enterprise from additional attacks after it became aware in March 2014 of a data breach whereby sophisticated adversaries targeted background investigation data.[436] The Committee obtained documents and testimony that show internal bureaucracy and agency politics trumped security decisions, and that swifter action by OPM to harden the defenses of its enterprise architecture by deploying Protect would have prevented or mitigated the damage that OPM's systems incurred.

OPM's "Cyber Climate" During Cylance Product Demonstrations

In June 2014, OPM began evaluating numerous products, including two Cylance products, for possible use in its legacy environment.[437] The agency's consideration of these tools occurred at a time when the agency was aware its existing environment had been compromised and vulnerabilities had been exploited by a sophisticated adversary.

On March 20, 2014, US-CERT notified OPM that data had been exfiltrated from OPM's system.[438] Agency officials later testified this data breach resulted in the loss of security documents and manuals about high-valued systems and applications on its enterprise architecture, but downplayed the significance of these documents.[439] US-CERT's June 2014 OPM Incident Report highlighted the sophistication of the attackers, which used "an extremely stealthy form of malware [a Hikit rootkit] designed to hide its malicious processes and programs from the detection of commodity intrusion detection and anti-virus products."[440] A rootkit is malicious piece of software that uses administrator or "root" access to modify system settings to hide malware and malicious code at lower layers of an operating system, rendering itself and adversary activity almost undetectable by common anti-malware software.[441]

From March 20, 2014 to May 27, 2014, OPM and US-CERT observed the attackers to learn more about their tactics, techniques, procedures (TTP's), and objectives – including the exfiltration of data.[442] In the final US-CERT June 2014 OPM Incident Report, US-CERT stated:

[436] Wagner Tr. at -92.

[437] McClure Tr. at 14.

[438] June 2014 OPM Incident Report at HOGR0818-001233.

[439] *Hearing on OPM Data Breach: Part II* (exchange between Chairman Jason Chaffetz and OPM Dir. Katherine Archuleta and OPM Chief Info. Off. Donna Seymour).

[440] June 2014 OPM Incident Report at HOGR081-001234; *see supra* Chapter 2 The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-related data

[441] *What is a Rootkit*, AVG available at: https://support.avg.com/SupportArticleView?l=en_US&urlName=What-is-rootkit.

[442] June 2014 OPM Incident Report at HOGR0818-001233.

> [T]he attackers primarily focused on utilizing [Server Message Block] commands to **map network file shares of OPM users who had administrator access or were knowledgeable of OPM's [Personnel Investigations Processing System] system**. The attackers would create a '**shopping list**' of the available documents contained on the network file shares. After reviewing the 'shopping list' of available documents, the attackers would return to copy, compress, and **exfiltrate the documents** of interest from a compromised OPM system to a [Command and Control] server.[443]

The discovery of a successful intrusion and data breach in the spring of 2014 put OPM on notice. Sophisticated attackers defeated their information security measures and practices, and remained unnoticed as far back as July 2012.[444] The attackers had a clear objective: the background investigation material contained in PIPS. In other words, OPM had every incentive to take swift, decisive action to immediately fortify its legacy systems against a persistent threat that already had secured an advanced understanding of OPM's environment, including its highest valued targets.

The agency purchased select tools from various vendors in June 2014,[445] but declined at this juncture to purchase a key preventative tool recommended by the OPM Director of IT Security Operations called CylanceProtect[446] and only bought its more limited tool, CylanceV.[447] The agency's security personnel remained interested in Protect, and Cylance arranged an extended demonstration in early 2015.[448] When OPM identified an indicator of compromise on April 15, 2015, the agency turned to Cylance for assistance.[449] As soon as OPM began using the Cylance tools in April 2015, it immediately began finding the most critical samples of malicious code on its network.[450] Cylance tools identified a significant amount of malware on OPM's network within 48 hours,[451] and Cylance personnel quickly recognized the agency's cyber situation was dire.[452] Cylance personnel even confided to each other internally over e-mail: "They are fucked btw."[453]

By April 2015, it was too late to undo the damage. Following the May 27, 2014 Big Bang, OPM decided not to purchase and deploy Protect as a result of internal bureaucratic

[443] June 2014 OPM Incident Report at HOGR081-001234-35.
[444] June 2014 OPM Incident Report at HOGR081-001235.
[445] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: Oct. 21, 2015) (on file with the Committee).
[446] Wagner Tr. at 91-92; *see also* McClure Tr. at 85-86.
[447] McClure Tr. at 19-20.
[448] *Id.*
[449] Coulter Tr., Ex. 2; E-mail from Matthew Morrison, Assurance Data, Inc., to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 10:48 p.m.) at HOGR020316-001899. (OPM Production: Apr. 29, 2016).
[450] Coulter Tr., Ex. 3; Saulsbury Tr. at 72; Email from [redacted] to Brendan Saulsbury, Senior Cyber Sec. Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).
[451] Coulter Tr., Ex. 3; Saulsbury Tr. at 72.
[452] McClure Tr., Ex. 9; Coulter Tr., Ex. 5.
[453] *Id.*

hurdles and "political challenges on the desktop."[454] The Big Bang remediation proved unsuccessful; the malicious actor linked to the theft of personnel records, background investigation data, and fingerprint exfiltration had already gained a foothold in OPM's system by May 7, 2014.[455] The malicious actor downloaded PlugX malware on May 7, 2014 on a key Microsoft SQL server[456] at OPM, and had moved laterally across the network to access the PIPS mainframe (which holds background investigation data) on or about June 23, 2014.[457] The attackers ultimately exfiltrated background investigation data from early July through August 2014, and then exfiltrated personnel records in December 2014 and fingerprint data in March 2015.[458]

Overview of the Cylance Cyber Tools

In June 2014, Cylance and OPM personnel began conversations about the potential use of Cylance's products in the agency's legacy (existing) information technology environment.[459] At this time, Cylance offered two products to the marketplace.

CylanceV (V) is a detection product used on end-point devices (i.e., desktop computers, laptops, etc.). First available to the marketplace in October 2013, V software scans endpoints to determine "whether or not something is malicious on a computer."[460] Deployment of V is limited to one endpoint at a time. The product is focused on detection—rather than prevention—of a cyber threat. Cylance CEO Stuart McClure testified that V "will find where an infection might already be or exist, and that will help IT operations to go into the computer, clean it up, fix it up, and do whatever they want to that system. But V is not preventive. It just is after the fact [it] will catch something."[461]

Protect, on the other hand, is designed to prevent malicious activity. It is distributed throughout an enterprise where it utilizes mathematics and algorithms to determine "good" from "bad." That is, it seeks to identify and address items that do not belong within an enterprise that could be a threat. The agency's threat detection and initial response efforts in the wake of the March discovery revolve, in part, around the two modes available through Protect: "Alert" and "Auto Quarantine."

In Alert mode, Protect places the onus on the administrator running the tool to determine whether or not Protect has identified a malicious computer process that should be quarantined, or if it should be "white listed" and remain operating on the environment. When

[454] McClure Tr., Ex. 4; McClure Tr. at 44-45.
[455] OPM Cybersecurity Events Timeline.
[456] June 2014 OPM Incident Report at HOGR0724-001154; OPM Cybersecurity Events Timeline.
[457] Coulter Tr. at 79-82, Ex. 18 (Email from Christopher Coulter to Jonathon Tonda); OPM Cybersecurity Events Timeline.
[458] OPM Cybersecurity Events Timeline; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); June 9, 2015 DMAR at HOGR0724-001158.
[459] McClure Tr. at 14 (The Cylance sales team was introduced to IT security personnel at OPM through Assurance Data. Cylance's sales staff, Nicholas Warner, was introduced to IT security personnel through Mathew Morrison at Assurance Data); McClure Tr. at 12-13 (Assurance Data maintained a re-seller arrangement with Cylance).
[460] McClure Tr., Ex. 1; McClure Tr. at 8.
[461] McClure Tr. at 8.

Protect is operating in "Auto Quarantine" mode, it automatically removes and quarantines threats, thereby requiring no intermediary action. McClure testified: "[Protect] sits on a computer in real time and watches everything that happens on a computer. And every single element of the computer determines whether it's good or bad, whether it's safe or unsafe, malicious or not. And if it's malicious, it stops it. It blocks it. It doesn't even allow it to start. So true -- true prevention."[462]

According to McClure, V:

> [R]equires a user to actually hit a button that says point to this drive or point to this computer or this share, whatever, now hit scan. It requires a physical body to do something like that. Whereas, CylanceProtect, the agent, can be completely hands-free. . . . If you just set it into auto quarantine mode, just forget it. If you have an alert mode, of course, then you have to review the alerts hopefully and then try and quarantine whatever things you find that are bad in there.[463]

April 15-16, 2015: The First 24 Hours

On April 15, 2015, OPM reported to US-CERT the first indicator of compromise.[464] This led to OPM's June and July 2015 announcements regarding the loss of 4.2 million personnel records, 21.5 million background investigation, and 5.6 million fingerprints. At this time, OPM owned V, but had not yet purchased Protect.[465]

OPM Director of IT Security Operations Jeff Wagner described how malware was discovered in 2015. Wagner testified that an indicator was found, then it was followed back to an infected server, and then the search began for the malware on the infected server.[466] Wagner testified:

> [T]he initial malware discovery on an infected machine is normally not done by, say, a tool. It's done once you find an indicator and that indicator points back. Then you use a tool such as Mandiant or Carbon Black or Cylance or various tools to do an overall search, because once you find one piece and you get additional indications, you can then look for other indications as well.[467]

Wagner testified that the unknown SSL certificate was "discovered by Websense" and that "Cylance would have found the specific malware on the machine. And then one of the engineers would have reverse engineered the malware to find it written within the malware."[468]

[462] McClure Tr. at 8-9.
[463] McClure Tr. at 46-47.
[464] June 9, 2015 DMAR at HOGR0724-001154.
[465] McClure Tr. at 20.
[466] Wagner Tr. at 54.
[467] Wagner Tr. at 54-55.
[468] Wagner Tr. at 80.

On June 17, 2014, the agency purchased an upgraded version of Websense[469] to replace an older Websense to "enhance the capability to include protection of remote users while attached to foreign networks."[470] Documents show the upgrade started on September 9, 2014 and was completed by September 17, 2015.[471]

By April 2015, OPM's IT Security Operations began to deploy the upgraded version of Websense and during this deployment process identified an initial indicator of compromise.[472] Saulsbury testified:

> We originally detected [a problem] during the course of the Websense rollout as we were sending groups of users, adding more and more groups of users to the pilot group, to have all of their outbound traffic being filtered through Websense. One of the things that we were doing was SSL decryption. Because that is such an intrusive method of inspection, we were monitoring for errors with SSL certificates that were potentially breaking access to applications, updates, and things like that.[473]

Saulsbury continued to describe the findings while rolling out Websense saying:

> [W]e also looked at the IP [sic] domain resolved to and put it into NetWitness. We were able to see that going back we had these three machines that were going through Websense, but we also had three servers that had been contacting this IP address. It looked very strange because there wasn't any business connection between these users' work stations and these three different servers. So that is when the red flag started to go up as this could potentially be malicious activity.[474]

At 6:53 p.m. on April 15, 2015, OPM's Computer Incident Readiness Team (OPM-CIRT) filed a report, INC478069, with US-CERT, and it was assigned incident number INC000000459698.[475]

[469] *Raytheon|Websense is Now Forcepoint*, FORCEPOINT, available at: https://www.forcepoint.com/raytheonwebsense-now-forcepoint, ("On January 14, 2016, Raytheon | Websense® announced that it was rebranding the product Forcepoint™ as part of a new venture between Raytheon and Vista Equity Partners").

[470] List of Tactical Security Products (Imperatis Production: Oct. 21, 2015).

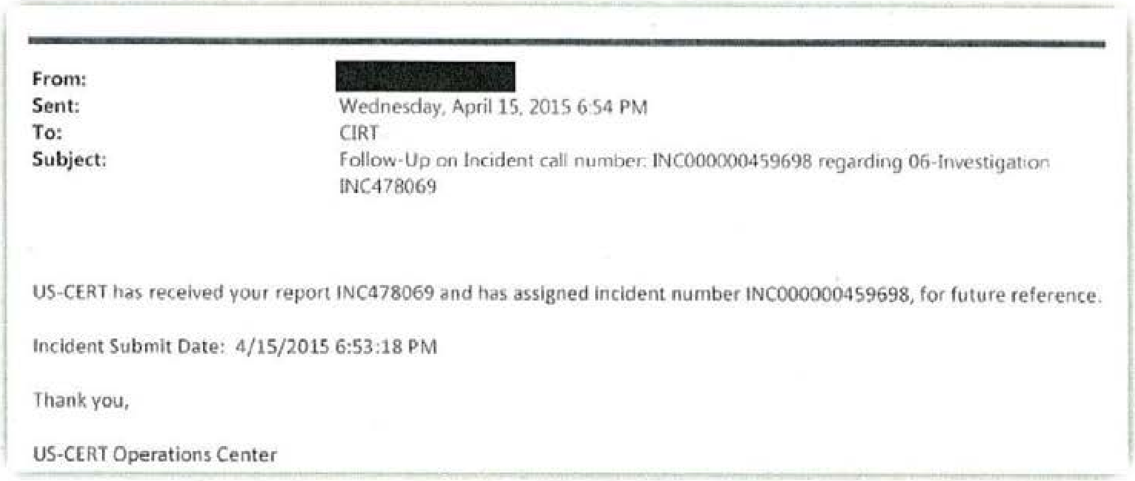
[471] *Id.*

[472] Saulsbury Tr. at 58.

[473] *Id.*

[474] Saulsbury Tr. at 59.

[475] E-mail from [redacted] to CIRT (OPM) (Apr. 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).



From: [redacted]
Sent: Wednesday, April 15, 2015 6:54 PM
To: CIRT
Subject: Follow-Up on Incident call number: INC000000459698 regarding 06-Investigation INC478069

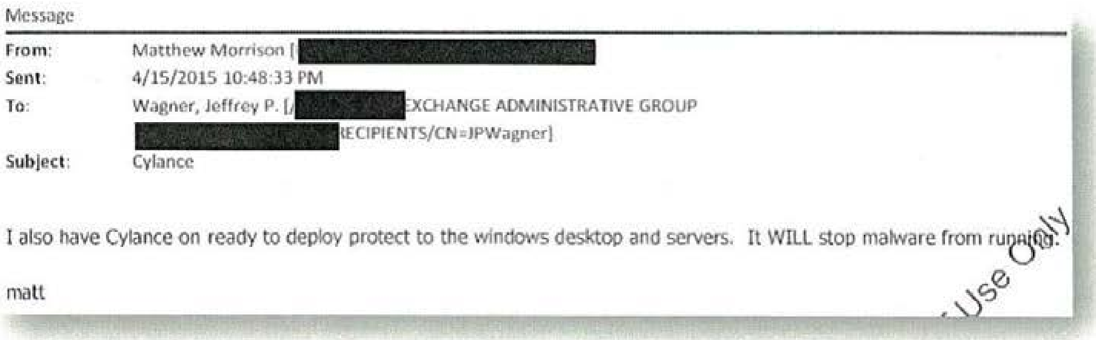
US-CERT has received your report INC478069 and has assigned incident number INC000000459698, for future reference.

Incident Submit Date: 4/15/2015 6:53:18 PM

Thank you,

US-CERT Operations Center

As OPM began to grapple with the developing cyber incident, the agency also discussed the possibility of using Cylance tools to stop the malware from functioning.[476] The documents show there was already a high degree of familiarity with the Cylance products and their capability, but that OPM did not have full access to the tools.[477]



Message

From: Matthew Morrison [[redacted]
Sent: 4/15/2015 10:48:33 PM
To: Wagner, Jeffrey P. [/[redacted]EXCHANGE ADMINISTRATIVE GROUP [redacted]RECIPIENTS/CN=JPWagner]
Subject: Cylance

I also have Cylance on ready to deploy protect to the windows desktop and servers. It WILL stop malware from running.

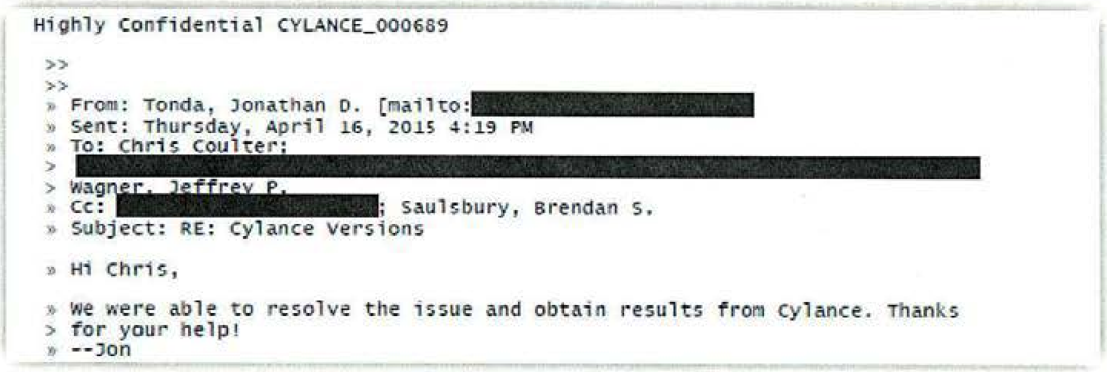
matt

As of the evening of April 15, 2015, OPM owned V, but did not have the latest version of V nor did OPM have access to Protect, the preventative tool.[478] The next morning (April 16) Cylance offered assistance to OPM as the agency was attempting to point V at endpoints, and soon thereafter provided technical support to OPM via conference call to help OPM overcome "incompatibility" issues.[479]

Chris Coulter, Cylance's Managing Director of Incident Response and Forensics, testified that "[OPM was] trying to use [V] against a forensic image, and the methods to do so aren't

[476] E-mail from Matthew Morrison, Assurance Data, Inc., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 10:48 p.m.), at HOGR020316-001899. (OPM Production: Apr. 29, 2016).
[477] *Id.*
[478] Coulter Tr., Ex. 2 (In this email, Matthew Morrison (with Assurance Data) wrote to Grant Moerschel (Cylance Sales Engineer), seeking the latest Cylance versions, copying Nicholas Warner (Cylance sales director), OPM personnel and OPM contractors, including Jeffrey Wagner (OPM Director of IT Security Operations)).
[479] Coulter Tr., Ex. 2; McClure Tr. at 65.

clearly documented because it's more of a trade craft to know how to do that."[480] Coulter offered to be onsite at OPM the following morning if the incompatibility issue with V was not resolved.[481] Jonathan Tonda (then an OPM contractor in IT Security Operations) replied: "We were able to resolve the issue and obtain results from Cylance. Thanks for your help!"[482]



```
Highly Confidential CYLANCE_000689

>>
>>
» From: Tonda, Jonathan D. [mailto:[redacted]
» Sent: Thursday, April 16, 2015 4:19 PM
» To: Chris Coulter;
> [redacted]
> Wagner, Jeffrey P.
» Cc: [redacted]; Saulsbury, Brendan S.
» Subject: RE: Cylance Versions

» Hi Chris,

» We were able to resolve the issue and obtain results from Cylance. Thanks
> for your help!
» --Jon
```

At 3:56 p.m., Saulsbury sent Wagner a list of four malicious executables identified by V that were residing on OPM servers, and each malicious executable was assigned a score under the Cylance rating system.[483] McClure described this rating system in his testimony to the Committee. He stated:

> So we rank and score files and executional elements in a spectrum from positive 1 to negative 1. Anything from a positive 1 to a zero is considered safe mathematically. Anything from zero to negative .8 is considered abnormal. And then from negative .8 to negative 1 is considered unsafe.[484]

Three of the four malicious executables found by V on April 16, 2015 were rated -1 and the fourth was rated -.93 on the Cylance scale.[485] Coulter testified that the files showed "That there's a potential for a breach or a compromise [past] a malware infection."[486] One of the four files included a Windows Credentials Editor (WCE). Coulter described the significance of the WCE finding:

> So malware, while, as nasty as it can be, is fairly common, at least in a broad sense. Somebody actually has to use that malware for it to be malicious, most of the time. When you see something like a confirmed Windows Credentials Editor of other types of credential dumping tools, **that's usually a sign of an overt act, so something that somebody with ill intent actually was trying to achieve** versus just a presence of a

[480] Coulter Tr. at 10-11.
[481] Coulter Tr., Ex. 2.
[482] *Id.*
[483] Coulter Tr., Ex. 3.
[484] McClure Tr., Ex. 87-88.
[485] Coulter Tr., Ex. 3.
[486] Coulter Tr. at 14-15.

> malicious file, which may or may not have been used. A WCE 64 doesn't just appear for -- just to have it there. It usually is used.[487]

US-CERT would later confirm WCE as a "hack tool."[488]

On April 15, OPM found another suspicious file—a McAfee dynamic link library (DLL) called "macutil.dll" that Saulsbury recalled in testimony as being integral to the attacks:

> So we took Cylance V and put it on the known infected machine with the McAfee macutil.dll malware -- so the machine with the mcutil.dll malware and then we ran Cylance V on it to scan the machine for malicious artifacts. And what it came up with is it successfully identified that mcutil.dll file as malware.[489]

The McAfee file was highly suspicious because OPM did not use McAfee in its systems. Saulsbury stated: "It was basically trying to fly under the radar as if it was a McAfee antivirus executable. The problem is that OPM doesn't use McAfee, so that stood out right there to us that, at that point, I was 100 percent certain that this is malware that is beaconing out."[490] The next day, US-CERT confirmed the malicious nature of this file.

April 17, 2015: US-CERT Confirms PlugX

On Friday, April 17, 2015 at 11:39 a.m., Saulsbury processed a new malware submission to US-CERT for its review that included the files he shared with Wagner the night before.[491] At 5:19 p.m., US-CERT reported to OPM its initial analysis of the executable files.[492]

US-CERT reported that the mcUtill.dll was a "loader"—an operating system component that copies programs to memory. When executed by a seemingly innocuous executable (mcsync.exe), mcutill.dll decrypts, decompresses, and loads a third file into memory (mcsync.eal). This file is the primary file – or payload – for a remote access tool (RAT) called PlugX. Each of these files was contained within a "McAfee.SVC" folder, which also contained an output file for the keylogger ([redacted]). PlugX used the malicious domain "wdc-newsport.com" for command and control.[493]

In other words, the four files contained in the folder, which resided within a directory called "[redacted]" worked in concert to harm OPM, and did so in a way that was hard to detect. Each of the four files had a specific function:

[487] Coulter Tr. at 16.

[488] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357 (April 17, 2015) at HOGR0092 (OPM Production: Dec. 22, 2015).

[489] Saulsbury Tr. at 66.

[490] Saulsbury Tr. at 60; email from [redacted] to Brendan Saulsbury, Contractor OPM IT Security Operations (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[491] Email from [redacted] to Brendan Saulsbury, Contractor OPM IT Security Operations (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[492] *Id.*

[493] *Id.*; June 9, 2015 DMAR at HOGR0724-001157.

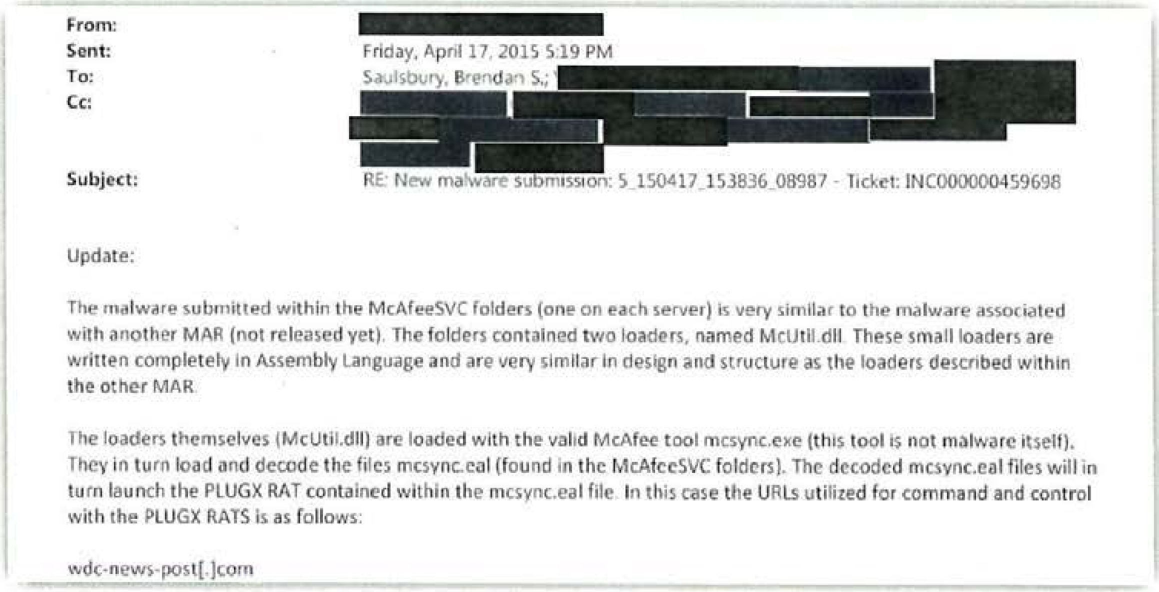
- Mcsync.eal is an encrypted .dll file and PlugX malware considered malicious. After analysis of the Master File Table (MFT), US-CERT found that the file was time-stamped. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- Mcsync.exe is a binary itself and is innocuous; however, it is used to load the PlugX malware through McUtil.dll. Analysis of the MFT shows the file was time-stamped. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- McUtill.dll is a binary that has been identified as a PlugX loader. It attempts to connect to the malicious domain "wdc-news-post[.]com" which resolves to IP [redacted] US-CERT found the attacker time-stamped the file. Documents show the creation date was March 9, 2015 at 6:13:01 a.m.

- Adb.hlp was found to be the output file created to store the key strokes recorded by mcsync.eal. In addition to key-logging, this version of PlugX is capable of remote access control, file/directory/drive enumeration, file/directory creation, process creation, enumerating the host's network resources, and establishing a SSL connection to malicious domains.[494]

US-CERT reported PlugX was located in two OPM directories: a McAfee folder ("[redacted]") and a directory called ("[redacted]").[495]



From: [redacted]
Sent: Friday, April 17, 2015 5:19 PM
To: Saulsbury, Brendan S.; [redacted]
Cc: [redacted]
Subject: RE: New malware submission: 5_150417_153836_08987 - Ticket: INC000000459698

Update:

The malware submitted within the McAfeeSVC folders (one on each server) is very similar to the malware associated with another MAR (not released yet). The folders contained two loaders, named McUtil.dll. These small loaders are written completely in Assembly Language and are very similar in design and structure as the loaders described within the other MAR.

The loaders themselves (McUtil.dll) are loaded with the valid McAfee tool mcsync.exe (this tool is not malware itself). They in turn load and decode the files mcsync.eal (found in the McAfeeSVC folders). The decoded mcsync.eal files will in turn launch the PLUGX RAT contained within the mcsync.eal file. In this case the URLs utilized for command and control with the PLUGX RATS is as follows:

wdc-news-post[.]com

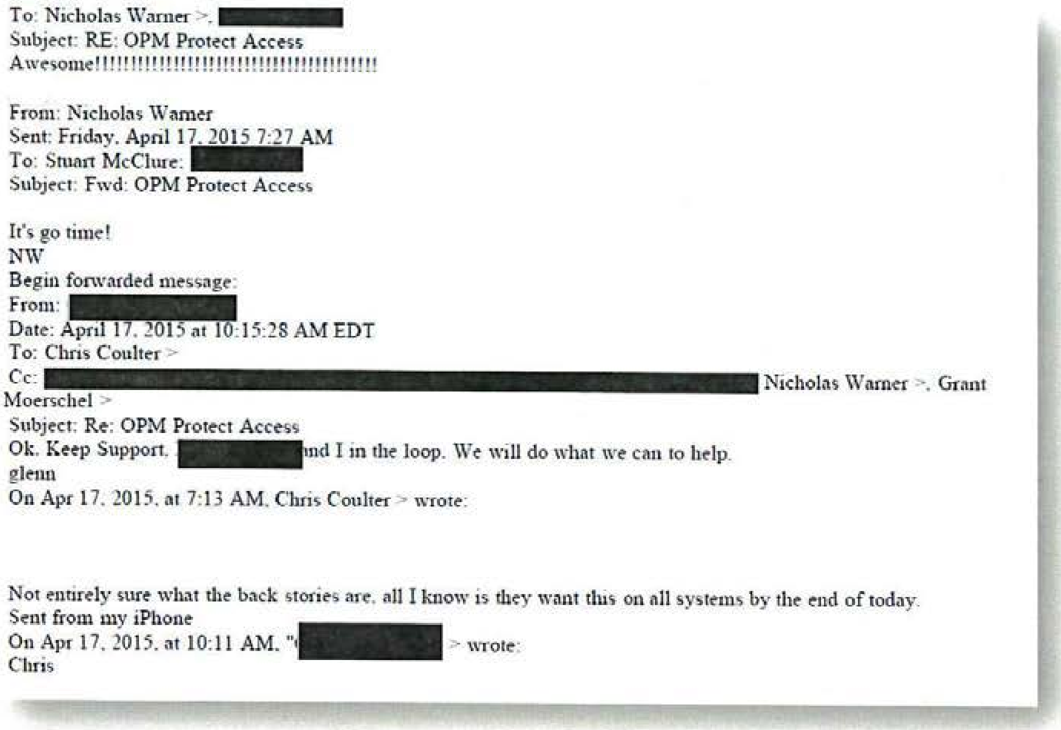
[494] June 9, 2015 DMAR at HOGR0724-001154. A US-CERT *Digital Media Analysis Report* provides detailed analysis and insight into the specific tactics, techniques, and procedures (TTPs) observed on the media submitted for analysis.

[495] June 9, 2015 DMAR at HOGR0724-001155.

April 17, 2015: CylanceProtect Deployed

On April 17, 2015, Coulter arrived at OPM's headquarters in Washington, D.C., to provide on-the-ground assistance.[496] That day, OPM decided to deploy Protect, but only in "Alert" mode (not in auto-quarantine mode).[497] Since OPM had been familiar with the product since June 2014, but still did not execute a purchase, Cylance staff was skeptical about whether this time the agency was truly moving to purchase and deploy Protect.

Cylance sales engineer Grant Moerschel emailed Coulter: "Is this a [Proof Of Concept] in their mind or the start of a real deployment?"[498] Coulter replied: "Not entirely sure what the back stories are, all I know is they want this on all systems by the end of today."[499] Director of Sales Nick Warner replied: "It's go time!"[500]



To: Nicholas Warner >, [redacted]
Subject: RE: OPM Protect Access
Awesome!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

From: Nicholas Warner
Sent: Friday. April 17. 2015 7:27 AM
To: Stuart McClure: [redacted]
Subject: Fwd: OPM Protect Access

It's go time!
NW
Begin forwarded message:
From: [redacted]
Date: April 17. 2015 at 10:15:28 AM EDT
To: Chris Coulter >
Cc: [redacted] Nicholas Warner >. Grant Moerschel >
Subject: Re: OPM Protect Access
Ok. Keep Support, [redacted]nd I in the loop. We will do what we can to help.
glenn
On Apr 17. 2015. at 7:13 AM. Chris Coulter > wrote:

Not entirely sure what the back stories are. all I know is they want this on all systems by the end of today.
Sent from my iPhone
On Apr 17. 2015. at 10:11 AM. "[redacted] > wrote:
Chris

OPM's Director of IT Security Operations, Jeff Wagner, testified that "we initially started using Cylance V for malware analysis. Within a day or two, we obtained the Protect. It was part

[496] Coulter Tr., Ex. 2; *see also* OPM Visitor Log Washington, D.C. (April 1, 2015 to July 10, 2015) at HOGR020316-000518 (OPM Production: Feb. 16, 2016).
[497] Coulter Tr., Ex. 17.
[498] McClure Tr., Ex. 6.
[499] *Id.*
[500] *Id.*

of our license, I believe."[501] As of April 17, 2015, OPM had not purchased a Protect license and did not purchase such as license until June 30, 2015.[502]

Nonetheless, Cylance provided OPM full access to Protect in mid-April 2015 on a demonstration basis and without purchasing a license because as Cylance testified it was evident OPM was under attack and they deemed it the appropriate course of action. McClure testified:

> A. Yes. So typically, like we say, an evaluation of this sort would be a small evaluation. However, when it's under these kind of incident response emergency situations, we allow them to install on as many boxes as they want. Because we just want to help them, provide them the support, get them to be able to identify the problems and then prevent them, clean it as quickly as humanely possible, get the bad actors out of the company, organization. So we allowed them to install on all of them, as many systems as they had -- a little unusual for an evaluation but not completely unusual, especially under these circumstances.
>
> Q. Those circumstances being?
>
> A. That **they were under severe attack and had been for quite some time.**
>
> Q. And you just described incident response efforts going on. Are you aware of the sense of urgency in how OPM was responding to what they found and flagged for your attention the day before?
>
> A. Once we were engaged on April 16th, 17th, it was very much a fire drill, every 24 hours. And they were taking it very, very seriously from all of our observations, and reacting as quickly as possible, and getting as much help as they could, and engaging with us, and getting the technology out there, and trying to quarantine as quickly as possible. It's actually one of the poster-child examples of how to do it properly in an investigation, just as soon as you humanely possibly know that you've been breached, to try and roll out this new tech. I think they did an admirable job.[503]

With respect to why OPM utilized Cylance tools in April 2015, Wagner testified:

> We were uncomfortable with just trusting that we knew all the indicators of compromise. And so we obtained the Cylance endpoint client and

[501] Wagner Tr. at 95.

[502] McClure Tr., Ex. 1; *see also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015), at CYLANCE 000018 (Cylance Production: Dec. 17, 2015).

[503] McClure Tr. at 58-59.

> deployed it, and then a Cylance engineer helped make sure we got it configured correctly to get proper information out of it."[504]

Wagner also testified that Cylance was able to find things other tools could not "because of the unique way that Cylance functions and operates. It doesn't utilize a standard signature of heuristics or indicators, like normal signatures in the past have been done, it utilizes a unique proprietary method."[505]

April 18, 2015: Protect Lights Up Like a Christmas Tree

On April 18, 2015, one day after deploying Protect, OPM rapidly escalated its use throughout the enterprise. McClure wrote: "I checked in on the deployment and we are at 2226 devices at last count. Tons of findings. Chris is working through them already quarantining. It is juicy."[506] McClure testified: "[**W]e were finding a ton of malicious attacks** on -- on the boxes that we were getting deployed to."[507]

On April 18, however, OPM was not yet utilizing Protect's full capability. The agency was using the product in "alert" mode and not "auto quarantine" mode.[508] Agency personnel therefore had to determine what should be stopped from operating in OPM's environment after reviewing alerts. When McClure stated in the April 18th email that "Chris is working through them…", this statement describes the steps that must be taken to evaluate each item OPM was alerted to before agency personnel could then consciously address them (i.e., extracted from the environment, white listed, etc.). McClure testified that **only about ten percent of Cylance's customers use the alert-only mode** and in alert-only mode, the product "will alert only when an attack is present or happening in the system."[509]

Wagner testified that OPM was running Protect in "passive mode, because we didn't want the tool to automatically end up deleting forensic evidence that we needed."[510] That is not how Protect works. McClure testified: "[W]hen we quarantine a file, we don't actually delete it yet. The rationale is, if we quarantine something by mistake, that's a false positive. In that rare instance, the customer would want to unquarantine it to put it back in production. So we keep it in a secure, untamperable space on disk that allows us to perform that unquarantining. Unfortunately, that does take up space as part of the quarantine area."[511]

Protect identified 39 "Trojans" on various parts of OPM's network that were rated a negative one (-1) on the Cylance rating scale—the worst possible rating—and Cylance staff recommended quarantining these items.[512] The finding of 39 Trojans was significant because as Coulter testified the "Trojan's" functionality allows the attacker to "bypass to some degree

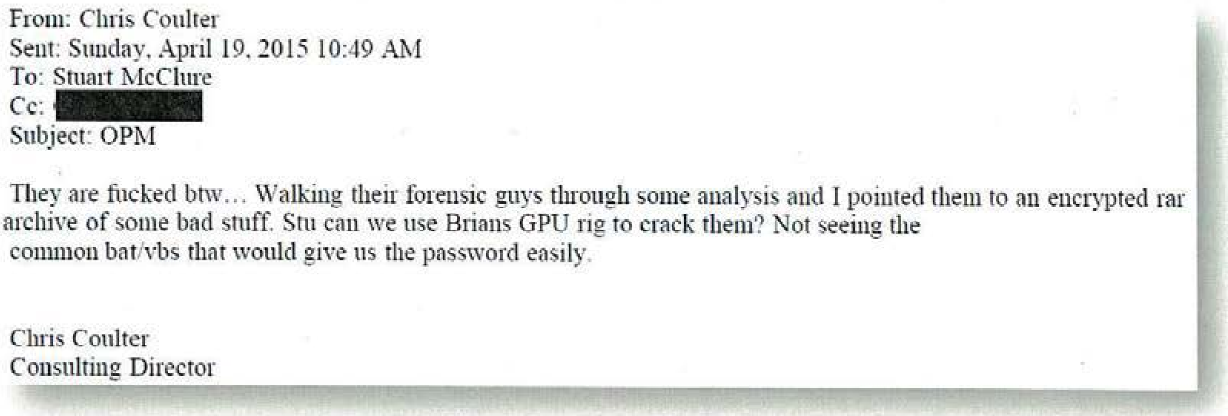
[504] Wagner Tr. at 87-88.
[505] Wagner Tr. at 96.
[506] McClure Tr., Ex. 8.
[507] McClure Tr. at 25.
[508] McClure Tr., Ex. 8.
[509] McClure Tr. at 10-11.
[510] Wagner Tr. at 94.
[511] McClure Tr. at 71.
[512] Coulter Tr., Ex. 4.

security controls and allow a bad actor, in some cases, unrestricted access to a network."[513] Coulter stated: "Any one Trojan could have that capability."[514]

In fact, when reviewing the work ticket that identified these 39 Trojans, Coulter testified: **"To say it bluntly, [Protect] lit up like a Christmas tree.**"[515] According to Coulter, Cylance's team concluded these were downloader files, which are typically associated with malware and multiple Trojans.[516] When asked these results caused concern, Coulter stated: "**Having gone through security clearance process many times, I know what OPM does. And dealing with APT almost on a daily basis, you put two and two together. You can just assume the risk that, you know, what could unfold or what could be there.**"[517]

April 19, 2015: Severity of the Situation Becomes Clear

It quickly became clear to Cylance that the IT security situation at OPM was dire. [518] By April 19, 2015 malicious items continued to be found in OPM's enterprise.



From: Chris Coulter
Sent: Sunday, April 19, 2015 10:49 AM
To: Stuart McClure
Cc: [redacted]
Subject: OPM

They are fucked btw… Walking their forensic guys through some analysis and I pointed them to an encrypted rar archive of some bad stuff. Stu can we use Brians GPU rig to crack them? Not seeing the common bat/vbs that would give us the password easily.

Chris Coulter
Consulting Director

In an April 19 email, Coulter reported to McClure that he had identified "an encrypted rar archive of some bad stuff." McClure told the Committee a "RAR" file is "a compressed encrypted archive of other files" that he recalled "seeing evidence of an attack that had already been there, been successful, and it was nasty" and that "[t]here were signs of ex-filtration of data, yes."[519] In order to address the "encrypted rar archive" finding, Coulter asked for assistance with another tool to help break the encryption. McClure testified:

> [W]hen forensic folks like us get on-site and take a look at these things, we can't easily open them and see what they've been able to steal and push out of the environment without using something like a GPU [Graphics Processing Unit] password-cracking rig, which is what's

[513] Coulter Tr. at 50.
[514] Coulter Tr. at 80.
[515] Coulter Tr. at 20-21.
[516] Coulter Tr. at 20-21.
[517] Coulter Tr. at 21.
[518] McClure Tr., Ex. 9; Coulter Tr., Ex. 5.
[519] McClure Tr. at 27.

> referenced here. . . So he's saying, you know, I'm not seeing the common BAT or VBS files that would give us the passwords easily. So typically, BAT is short for batch files, and they are Windows batch files. And VBS is short for visual basic scripting or script, both of which help automate certain commands that are run on a computer system. And oftentimes, because hackers are lazy, they'll put into the batch or the VBS scripts, the actual hard-putted password of the encrypted RAR, so that they can help automate both encryption and decryption of it in their tasks.[520]

On April 19, the signs of a significant compromise at OPM were clear. Coulter testified:

> They're in a severe situation. . . . It's an incident now. It's much more than just a malware incident. So when I was talking earlier about, you know, credential dumping tools and overt actions, **this is again another overt action**. If you don't usually -- if you can't explain why you have a large encrypted RAR archive in a location that most administrators would recognize, there's -- it's likely a stash of something.[521]
>
> * * *
>
> So as is common in a lot of APT cases, or actually a lot of breaches, if their end goal is to collect data, then they're going to search for it and bring it back to a central point for aggregation. A lot of times data, like this email, if you were to compress it, it would be, you know, potentially one-100th of the size. So RAR, which is a compression format, is used to shrink data. You can also then apply a password to it. So in a lot of cases, where there is data exfiltration or a confirmed breach, it's very common to find these compressed, encrypted stashes of whatever bad guys were after.[522]

Like McClure, Coulter also testified that, as of April 19, 2015, a significant chance existed that data from OPM had been exfiltrated.[523] US-CERT's analysis validated their concerns. According to US-CERT:

> Analysis of the image revealed that several variants of PlugX once resided on the victim machine, with the last variant from downloaded folder RAR SFX2 still residing. Several password protected RAR files were found on the victim machine which have been identified by the customer as exfiltrated data.[524]

[520] McClure Tr. at 27-28.
[521] Coulter Tr. at 25-26.
[522] Coulter Tr. at 26-27.
[523] Coulter Tr. at 27.
[524] June 9, 2015 DMAR at HOGR0724-001156.

RAR Files

A Roshal Archive or RAR file is a means to compress and encrypt data, which facilitates moving large amounts of data more easily and securely. Compression diminishes network footprint and encryption concealed contents of malicious files or stolen data, making it more difficult for security software to detect the malicious actors' activities.

RAR files have three notable qualities that help explain their usage in the 2015 data breach:

(1) Compressed – the overall file size is reduced and simplified, allowing it to take up less space on disk and making it easier to move around OPM's internal systems, and exfiltrated from its network.
(2) Encrypted – the contents of the RAR files are obfuscated, hidden beneath layers of encrypted code; and conceal their contents.
(3) Unpackability – when executed, RAR's "extract" their contents, creating a directory to place the files they compress and encrypt.

The three variants of PlugX malware used in the 2015 data breach can be tied to RARSFX0, RARSFX1, and RARSFX2 respectively, and give forensic investigators clues as to where the attackers were on OPM's systems and when.

The RAR files that had been identified were notable because these files were ultimately linked to the data exfiltration of the background investigation and fingerprint data and personnel records. For example, RAR SFX2 appears to contain FTS data held on the attackers' primary foothold – WDC-new-post.com.[525] Another, RAR SFX2, when downloaded created the "McAfeeSVC" folder in a directory ("[redacted]") located on a key Microsoft SQL server [redacted][526] and its duplicate server [[redacted]]. This location gave attackers access to a key jump box that facilitated access to other segments of OPM's environment—segments that house sensitive information.[527] US-CERT found the attacker was active on that server stating: "the first appearance by the actor that was observed on the victim images was on 5/7/2014 at 11:12:25PM from a SQL Server."[528]

US-CERT's analysis of this string of malicious activity would later point out the liability to the country: "It is interesting to note the machine had an [remote desktop protocol] session with [United States Government [redacted] system [redacted] on 10/22/2014."[529] In other words, US-CERT was pointing out a remote desktop session that occurred in October 2014 on the system that led to a tunnel (Interior Business Center) at the Department of Interior (DOI) and to the federal employee personnel records that were stolen. US-CERT and OPM would later affirm that the attacker pivoted to the data center at DOI in October 2014, with the personnel records subsequently being exfiltrated in December 2014.[530]

In an exchange with Rep. Robin Kelly (IL), DOI's CIO, Sylvia Burns would later testify before the Committee about how the attacker traversed onto DOI's network and stole the personnel records:

> Ms. KELLY. Thank you, Mr. Chairman. Ms. Burns, the two data breaches OPM recently reported have been particularly concerning to us because of the national security risk involved. According to testimony you

[525] June 9, 2015 DMAR at HOGR000092-93.
[526] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at 000090 (US-CERT Production: Dec. 11, 2015).
[527] Saulsbury Tr. at 74-75.
[528] June 9, 2015 DMAR at HOGR0724-001154.
[529] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at 000090 (US-CERT Production: Dec. 11, 2015).
[530] OPM Cybersecurity Events Timeline.

> gave at a recent hearing on the OPM data breaches, the OPM personnel records that were compromised in one of those breaches were hosted in the data center maintained by the Department of Interior. Did the cyber attackers who gained access to those records also gain access to the Interior Department data center?
>
> Ms. BURNS. So the adversary had access to our data center. It was exposed. There was no evidence based on the investigation that was led by DHS, US–CERT, and the FBI, there was no evidence that the adversary had compromised any other data aside from the OPM data.
>
> Ms. KELLY. Okay, so the same cyber intruder who breached OPM's personal data, which the Department of Interior hosted on its servers, also breached the defense's of the Interior Department data center?
>
> Ms. BURNS. So this, the intrusion that you're referring to, was a sophisticated breach. And my understanding, based on DHS' assessment, was that the adversary exploited, compromised credentials on OPM's side to move laterally and gain access to the Department of Interior's data center through a trusted connection between the two organizations.
>
> Ms. KELLY. So the cyber intruder, did they gain access it to DOI's data center through OPM or was it the other way around?
>
> Ms. BURNS. The adversary gained access to DOI's infrastructure through OPM, as far as I understand, based on DHS's investigation.
>
> * * *
>
> Ms. KELLY. In addition to hosting OPM's personnel records, the Department hosts data from other agencies in its data center. Is that correct? And, if so, which agencies?
>
> Ms. BURNS. Yes. Actually, the Department is a—the data center in question, the biggest customer of the data center is actually Interior. So it's the Interior Business Center, what we call IBC. They're a shared service provider, and they are the majority user of the data center. And we also host some applications for the Office of the Secretary in the data center.[531]

The same day RAR files were being discovered (April 19, 2015), Protect also identified "command shells."[532] Command shells are significant because they provide a means for the attacker to remotely control a victim machine. On April 19, 2015, McClure wrote to Coulter:

[531] *Cybersecurity: The Department of the Interior: Hearing Before the Subcomm. on Information Tech. and Subcomm. on Interior of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 21-22 (July 15, 2015).
[532] McClure Tr. at 31; Email from Stuart McClure, Chief Exec. Officer, Cylance to Chris Coulter, Managing Dir., Cylance (Apr. 19, 2015, 9:01 p.m.), at CYLANCE_002112 (Cylance Production: Jan. 27, 2016).

"They quarantined one of the xCmd.exe files but I found two more. Might want to recommend they quarantine those too."[533] McClure explained the significance of finding "xCmd.exe files:"

> A. Sure. So XCMD -- so CMD stands for command, and they usually stand for command shells. And what that allows you to do is actually have remote access of their computer on your own computer. So **when you start XCMD on the victim box, it will then create a shell to you on your remote computer, wherever you are in the world, and you can then type commands as if you are sitting right there on the computer**.
>
> Q. And why did you recommend quarantining another two mentioned in the message?
>
> A. Because that's -- **that's as nasty as you can get. I mean, they can do anything that they want with that access.**[534]

Cylance and OPM made additional findings about the breach on April 19, 2015.[535]

Then on April 20, 2015, a Cylance expert contacted Coulter about OPM data collected and a "backdoor." Thus, began a chain of events eventually leading to the discovery background investigation data had been stolen. Specifically, the Cylance expert wrote to Coulter:

> Give me a call when you have some time. I'm going through the data now. Wanted to ask some questions about the system WCE was sitting on and a few others. You may want to have them get an image of [__] is **a backdoor that looks like the [command and control server] was active around 6/2014** corresponding to when they came out and said they had a problem. Callback was to resolved to if they have any kind of network or DNS logs going back that far.[536]

This communication in particular would start the process of revealing how the background investigation materials were compromised. More evidence would unfold and become clear in the coming days.

[533] McClure Tr. at 29; Email from Stuart McClure, Chief Exec. Officer, Cylance to Chris Coulter, Managing Dir. of Incident, Cylance (Apr. 19, 2015, 9:01 p.m.), at CYLANCE_002112 (Cylance Production: Jan. 27, 2016).

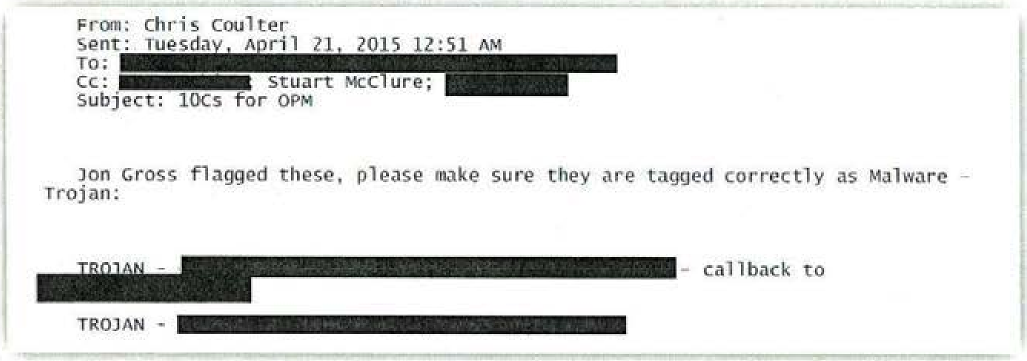
[534] McClure Tr. at 29-30.

[535] The same day that Cylance identified RAR files and was working to decode the passwords, Protect found "a fraudulent attempt at making this look like a Bit9 signed binary. See the signed by "Bit89 Inc."? And [website Virus Total] calls it quite evil." McClure Transcribed Interview, Ex. 10. VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, Trojans and other kinds of malicious content detected by antivirus engines and website scanners. *About Virus Total*, VIRUS TOTAL available at: https://www.virustotal.com/en/about/.

[536] Coulter Tr., Ex. 6.

April 20-23, 2015 – More Key Trojans Identified; OIG First Notified.

The agency continued to expand its use of Protect through April 21, 2015. The tool was on 6,725 hosts and it was expected to roll out to 10,000 hosts soon thereafter.[537] On April 21, Cylance also identified two Trojans sitting on key servers.[538]



From: Chris Coulter
Sent: Tuesday, April 21, 2015 12:51 AM
To: [redacted]
Cc: [redacted]; Stuart McClure; [redacted]
Subject: IOCs for OPM

Jon Gross flagged these, please make sure they are tagged correctly as Malware - Trojan:

TROJAN - [redacted] - callback to [redacted]

TROJAN - [redacted]

At that point, OPM also began utilizing more outside help. CyTech's CyFIR Enterprise was installed on the servers where Coulter had identified new pieces of Trojan malware.[539] CyTech's CyFIR then imaged malware and artifacts residing on these servers that were subsequently supplied to US-CERT. Those findings were covered in US-CERT's May 4, 2015 "Preliminary Digital Media Analysis Report" and June 9, 2015 "Digital Media Analysis Report."[540]

Cylance also discovered remnants of malware used by adversaries in the 2014 intrusion against OPM. CylanceProtect found "dormant" variants of Hikit, which was the primary malware used by the attackers discovered in 2014, on OPM's systems during the discovery phase of the 2015 investigation. Jeff Wagner, OPM's Director of IT Security Operations, stated Cylance. "In doing a full analysis of the entire network…did find an older version of Hikit. It also found library fragment files of malware."[541] Wagner testified regarding the Hikit malware found by Cylance and its relevance to the 2015 intrusion:

> A. So the Hikit variant discovered in 2015 was not an active piece of malware, it was a dormant piece of malware. That because Cylance was utilized to analyze the entire environment, we discovered the malware was dormant within one of the servers. It was believed to have been an abandoned piece of malware that was previously installed at some other time.
>
> Q. Was it related to the incident in 2015?

[537] McClure Tr., Ex. 11.
[538] Coulter Tr., Ex. 7.
[539] Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[540] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis Report - INC465355-A (May 4, 2015), at HOGR_US-CERT_000346-48 (US-CERT Production: Dec. 11, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[541] Wagner Tr. at 126

> A. We don't have direct evidence it was necessarily related to the 2015 incident. It was discovered in the 2015 incident.
>
> * * *
>
> Q. Sorry. So did you have any indirect evidence that the [Hikit] found referenced in the 2015 DMAR was at all involved in the 2014 breach?
>
> A No. We don't believe…I don't remember the exact, quote, "born on date" of the malware, which shows the initial point of infection, but it was not during the 2015 timeframe of adversary activity. **So we really didn't have a recognized idea as to when it showed up**. It was one of those pieces of malware, as well as additional fragments of former malware that Cylance identified, and we proceeded to eliminate along with everything else.[542]

One of the two Trojans found on April 21 contained what US-CERT called a "unique"[543] file named winrsves.dll, with a compile time of 5:34:46 EST on March 18, 2011.[544] This file was a malicious Windows Dynamic Link Libraries (DLL) file designed to run as a service. When running, the DLL allows a hacker to pass and execute encrypted executables and DLLs to a victim system at will.[545]

This first "unique" Trojan file (winrsves.dll) contained a "plugin" framework that allowed it to import and load DLL files. US-CERT described the file as follows: "The DLL [which is identified as a Hikit Remote Access Tool (RAR)] is unpacked and loaded into memory, while never being written to disk. During execution, this DLL will attempt to read a configuration file in the same folder in which it was executed. This configuration is expected to have the same name as the originally executed file, but with a *.conf* extension. In this case, the expected configuration file is winrsves.conf. If this file is not found, the malware will create a configuration file which contains its default configuration."[546] The CMD.exe[547] Cylance found on April 19 would reveal that the configuration file contains the command and control location [redacted] The configuration file contains the configuration string [redacted][548]

[542] Wagner Tr. at 134-135

[543] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-B (corrected) (April 24, 2015) at HOGR0724-001065 (OPM Production: Dec. 22, 2015).

[544] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis Report - INC465355-A (May 4, 2015), at HOGR_US-CERT_000348 (US-CERT Production: Dec. 11, 2015).

[545] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-B (corrected) (April 24, 2015) at HOGR0724-001065 (OPM Production: Dec. 22, 2015).

[546] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190 (US-CERT Production: Dec. 11, 2015).

[547] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190-91 (US-CERT Production: Dec. 11, 2015).

[548] June 9, 2015 DMAR at HOGR0724-001154 (This particular HiKit uses the same strong [redacted]" in the output configuration file as US-CERT found in DMAR 355170).

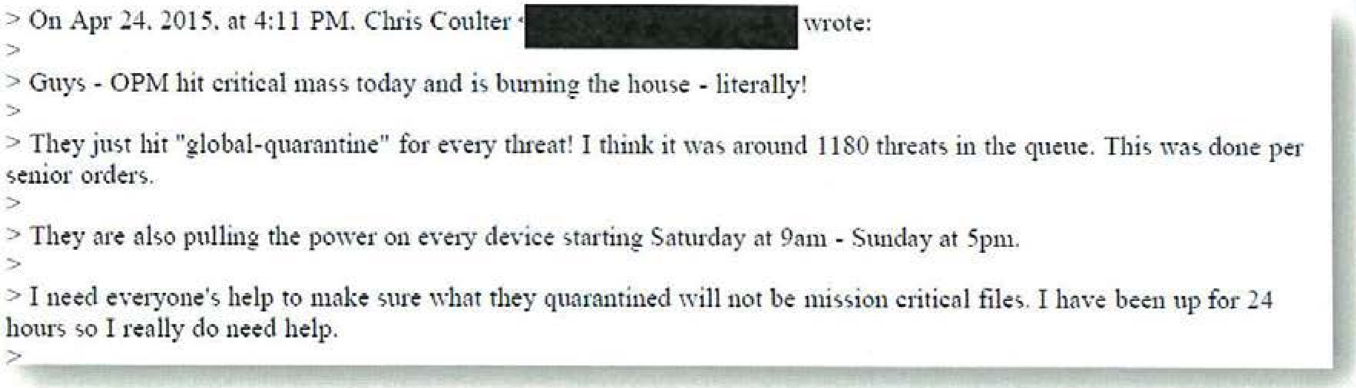
The second Trojan was located on a server [redacted] and was called "[redacted]." According to US-CERT this was a *Dropper.Generic9.TIC* Hikit found to have resided on the victim machine since September 15, 2012 at 07:07:53AM.[549] This binary also pointed to the malicious domain [redacted]"[550] The cybersecurity event that was developing at OPM was serious. It was not until April 22, 2015, however, that the agency notified the Office of the Inspector General that it was dealing with a breach.[551] In fact, the notification occurred entirely by accident.[552]

And while the Protect deployment was successfully identifying critical malicious items, the product was still being introduced into OPM's system conservatively. Protect was in Alert mode meaning threats were not automatically quarantined.[553] In addition, Protect was not yet on all OPM hosts. On April 23, 2015, Coulter emailed an OPM official: "Just letting you know we do not have Protect on the following key hosts [servers]."[554]

April 24-25, 2015 – OPM Upgrades Protect to Auto-Quarantine Mode.

On April 24, 2015, OPM upgraded Protect to auto-quarantine mode. At 4:11 p.m. on April 24, Coulter emailed several colleagues to announce the upgrade. He wrote:

> Guys - OPM hit critical mass today and **is burning the house** - literally! **They just hit 'global-quarantine' for every threat! I think it was around 1180 threats in the queue. This was done per senior orders.** They are also pulling the power on every device starting Saturday at 9am - Sunday at 5pm. I need everyone's help to make sure what they quarantined will not be mission critical files. I have been up for 24 hours so I really do need help.[555]



```
> On Apr 24, 2015, at 4:11 PM, Chris Coulter <[redacted] wrote:
>
> Guys - OPM hit critical mass today and is burning the house - literally!
>
> They just hit "global-quarantine" for every threat! I think it was around 1180 threats in the queue. This was done per
senior orders.
>
> They are also pulling the power on every device starting Saturday at 9am - Sunday at 5pm.
>
> I need everyone's help to make sure what they quarantined will not be mission critical files. I have been up for 24
hours so I really do need help.
>
```

[549] June 9, 2015 DMAR at HOGR0724-001173.
[550] *Id.*
[551] OIG Memo, *Serious Concerns*.
[552] *See Infra*, Chapter 7: OPM's CIO and its Federal Watchdog.
[553] McClure Tr. at 33.
[554] Coulter Tr., Ex. 8.
[555] McClure Tr., Ex. 12.

Prior to April 24, OPM manually considered whether each item that Protect flagged should be removed from the system. McClure testified:

> My recollection was [OPM was] processing all the alerts themselves, along with the help of us at Cylance, our alert management team, as well as Chris Coulter, myself and others, to help them triage and process the alerts to make sure that they are malicious and not safe, and just trying to empower OPM themselves to make the judgment call on whether to quarantine those files and move them out of alert-only.[556]

Thus, while Protect was operating in alert mode, the burden was on OPM staff to determine what files should be quarantined, or be allowed to remain operational in OPM's environment. McClure testified:

> Q. Can you define, when you said that OPM was processing things on their own, can you define "processing"?
>
> A. Yes. They were in our management console looking at each alert trying to understand if they should actually quarantine it, delete it, or just allow it to continue to be on the system and study it for whatever purpose.
>
> Q. So OPM was making the decision on what to delete out of the items identified prior to April 24th, 2015?
>
> A. Correct. All customers manage their own quarantine.[557]

Saulsbury, who was on site at OPM on April 24, 2015, provided similar testimony:

> So after we observed that Cylance V was able to detect the APT malware, in this case it was, in the 2015 incident it as a malware family called PlugX. And once we were able to determine that V was able to detect PlugX, at some point there was a decision made to deploy the Protect agent to all of OPM's machines.
>
> So that was done with the assistance of the vendor of Cylance. And so the guy that I am emailing on that is Chris Coulter. So Chris was really good about helping us getting Protect deployed throughout the environment and then also analyzing all the findings that it is coming back with. So Cylance is detecting not just the APT malware, but every type of malicious, like, adware toolbar that somebody downloads and things like that, as well as the false positives here and there.

[556] McClure Tr. at 34-35.
[557] McClure Tr. at 35-36.

> So Chris was really good about helping us triage through that list and separate what we want to quarantine versus what is false positive and whitelisted. So at a certain point we were confident enough that we had identified all of the malware and had whitelisted the business critical applications that needed to be whitelisted. And so Jeff instructed us to quarantine all of the identified findings.
>
> What that quarantine means is, so when Cylance detects something, we just had it in alert mode. **So it would see it and say, hey, this is bad, but it is just alerting us on it, it is not actually doing anything about it. So what we essentially did on April 24th was press a button in the Cylance console and says everything that you've seen that is bad, take that and quarantine it so it is not operable on the machine.**[558]

Wagner also confirmed that OPM quarantined all the identified malware on or about April 24, 2015. With respect to why the quarantine did not happen before April 24, 2015, Wagner stated:

> So once you identify malware functionality or adversary activity, you try to get a sense of the adversary's intention, activities, and exposure. You look to see how deep they are in the environment. So once you discover something on the 15th, we didn't want to just start shutting things off.
>
> We didn't understand the depth in which the adversary had been in the environment. With the deployment of the Cylance tool, a full accountability of all binaries, we had discovered, identified, and all the malware was placed into the quarantine queue by I think it was the 19th of April . . . . And by the 24th, we had a full understanding that it had discovered everything that was to be discovered, and we no longer necessarily needed the adversary to have an active presence within the environment. So we ordered Cylance to destroy the malware.[559]

The auto-quarantine did not apply to all of OPM's systems, however. For certain systems, OPM made a value judgment as to whether they should be included in the auto-quarantine, or remain subject to the human command quarantine in auto-alert mode. Coulter provided guidance to his colleagues at Cylance on April 24, 2015 regarding what files to quarantine. He wrote:

> I would say anything on desktops are ok to quarantine. Servers should be the only thing questioned at this point. If they can live without it keep it blocked. They are setting up some help desk protocols to identify issues that come out of this.
>
> Mission critical items that I know of:

[558] Saulsbury Tr. at 72-73.
[559] Wagner Tr. at 121-122.

> > USA JOBS related apps - **they said if we bring that down senators will come for us**
> >
> > LAN Desk / SCCM
> >
> > SQL/Oracle components and connectors to mainframes
>
> Past that they can live without for a few weeks. This is a desperate move, tomorrow is even more desperate by unplugging every device and moving over to new networks. They will blame any issues on the power outage ;).[560]

McClure testified that in auto-quarantine mode, mission-critical items may stay in "alert" mode so as not to undermine the system in the event of a false positive.[561] McClure also testified that OPM should have considered shutting down mission-critical items given the severity of what Cylance was finding. He testified, "Yes, they should be."[562]

Documents and testimony show OPM used Protect as its quarantine tool and that Protect was not put into auto-quarantine mode until April 24, 2015. Documents and testimony also show some OPM systems were not placed into auto-quarantine mode at all. Contrary to this evidence, OPM's leadership testified before the Committee in June 2015 that the quarantine was fully in place by an earlier date, and stated that the malware was "latent" and merely being observed.[563] The term "latent" means the malware is not active on the environment—it is frozen or otherwise not running on active computer processes. The quarantine status was not activated until April 24, 2015 when OPM gave Cylance the authority to place Protect into auto-quarantine mode.[564] Unless Protect is in "auto-quarantine" mode, malicious items are not latent—an action is required to stop malicious items from functioning in the environment.[565]

April 26 – April 30, 2015: First Signs of Lost Background Materials

According to Wagner, in the days that followed the deployment of Protect's auto-quarantine function, OPM had "discovered everything that was to be discovered,"[566] but significant discoveries continued. The new discoveries were noteworthy because they provided evidence related to the loss of background investigation materials.

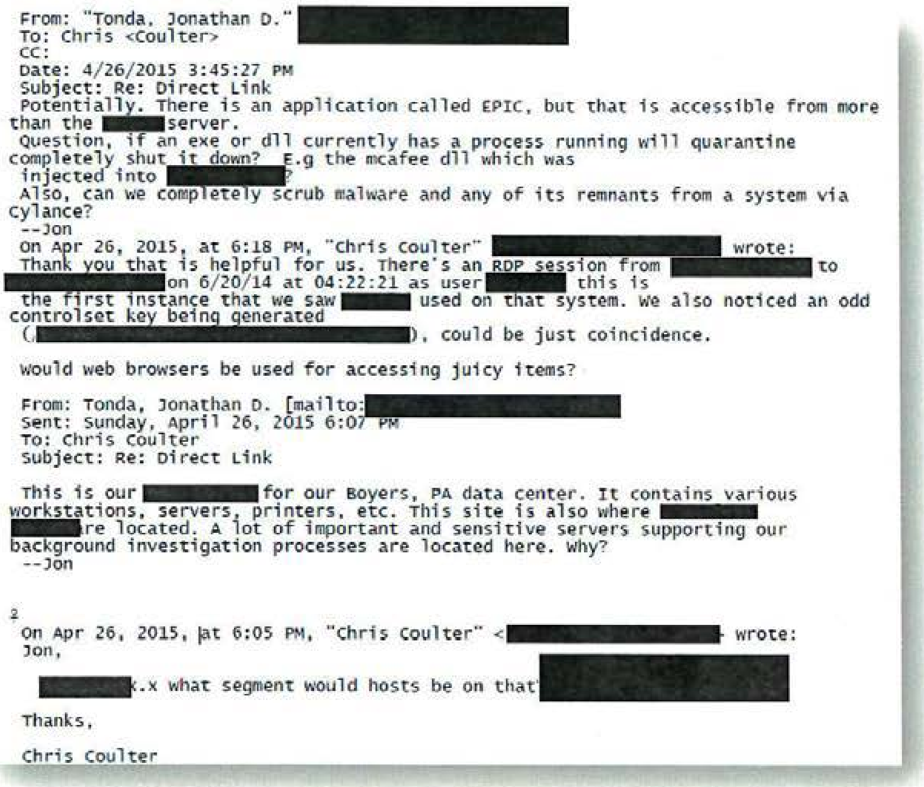
On April 26, 2015, Coulter and Jonathan Tonda (an OPM contractor at the time in OPM IT Security Operations) engaged in an email exchange about a segment of the OPM network.[567] This was the same segment that a Cylance expert asked Coulter to image on April 20 writing: "Give me a call when you have some time. I'm going through the data now. Wanted to ask some

[560] Coulter Tr., Ex. 17.
[561] McClure Tr. at 67.
[562] McClure Tr. at 68.
[563] *Hearing on OPM Data Breach: Part II* at 69; *see Infra,* Chapter 5: The CyTech Story for more on quarantine statements by OPM officials before the Committee.
[564] McClure Tr., Ex. 12; Coulter Tr. at 74-75.
[565] McClure Tr. at 34-36; Coulter Tr. at 34-36.
[566] Wagner Tr. at 121-122.
[567] Coulter Tr. Ex. 18.

questions about the system WCE was sitting on and a few others. You may want to have them get an image of [__] is **a backdoor that looks like the [command and control server] was active around 6/2014 corresponding to when they came out and said they had a problem.** Callback was to resolved to if they have any kind of network or [Domain Name System] logs going back that far."[568]

In this April 26 email exchange between Coulter and Tonda, Coulter was investigating a Remote Desktop Protocol (RDP) session that dated back to June 20, 2014 and accessed a particular segment of OPM's environment. Coulter asked Tonda what was hosted on the segment Coulter was investigating.[569] Tonda responded the segment Cylance identified was where ". . . [a] lot of important and sensitive servers supporting our background investigation processes are located."[570] **This was an important development because this server provided access to the PIPS mainframe – where background investigation data was stored.**[571] US-CERT/OPM would later confirm the "first known adversarial access to OPM's mainframe" as occurring June 23, 2014.[572]

[568] Coulter Tr., Ex. 6.
[569] Coulter Tr. Ex. 18.
[570] *Id.*
[571] Coulter explained in the email that the segment he had identified was a key "jump box" at OPM identified as [redacted] – a jumpbox means a server that manages access between two different network sections of the larger information technology environment (Saulsbury Tr. at 74-76). At OPM, this particular jumpbox enabled access to various parts of the OPM environment (Saulsbury Tr. at 74-76) and Cylance's Coulter was letting OPM know on April 26 that the jumpbox had a Remote Desktop Protocol (RDP) session to a significant server [redacted] that gave access to the portion of OPM's network where background investigations are stored (Coulter Tr., Ex. 18).
[572] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.



```
 From: "Tonda, Jonathan D." [redacted]
 To: Chris <Coulter>
 CC:
 Date: 4/26/2015 3:45:27 PM
 Subject: Re: Direct Link
 Potentially. There is an application called EPIC, but that is accessible from more
than the [redacted] server.
 Question, if an exe or dll currently has a process running will quarantine
completely shut it down?  E.g the mcafee dll which was
 injected into [redacted]?
 Also, can we completely scrub malware and any of its remnants from a system via
Cylance?
 --Jon
 On Apr 26, 2015, at 6:18 PM, "Chris Coulter" [redacted] wrote:
 Thank you that is helpful for us. There's an RDP session from [redacted] to
[redacted] on 6/20/14 at 04:22:21 as user [redacted] this is
 the first instance that we saw [redacted] used on that system. We also noticed an odd
controlset key being generated
 ([redacted]), could be just coincidence.

 Would web browsers be used for accessing juicy items?

 From: Tonda, Jonathan D. [mailto:[redacted]
 Sent: Sunday, April 26, 2015 6:07 PM
 To: Chris Coulter
 Subject: Re: Direct Link

 This is our [redacted] for our Boyers, PA data center. It contains various
workstations, servers, printers, etc. This site is also where [redacted]
[redacted] are located. A lot of important and sensitive servers supporting our
background investigation processes are located here. Why?
 --Jon


2
 On Apr 26, 2015, at 6:05 PM, "Chris Coulter" <[redacted] wrote:
 Jon,

   [redacted].x what segment would hosts be on that [redacted]

 Thanks,

 Chris Coulter
```

With respect to this jump box, US-CERT found another related directory infected with PlugX. US-CERT reported:

> Malicious binaries no longer reside on the victim machine, which has been identified as a jump server; however, analysis displays the system was once infected by malware. Remnants of malicious files were found in the directory [redacted] with PlugX files [redacted] [redacted], [redacted] and [redacted] located on image. Also metadata displays malicious domain opmsecurity[.]org found on image.[573]

As was the case with the McAfeeSVC directory that contained malware, this directory—[redacted]—contained four files: one output keylogger file; an innocuous file that PlugX used; and two binaries that were PlugX malware files.[574]

By the end of April, the situation at OPM began to stabilize and Cylance personnel prepared to leave the agency's headquarters. On April 29, 2015, Cylance reported to Wagner and others at OPM that "I will be working remote today as I think everything is resolved that would have required me to be onsite."[575]

[573] June 9, 2015 DMAR at HOGR0724-001155.
[574] June 9, 2015 DMAR at HOGR0724-001154.
[575] Coulter Tr., Ex. 14.

As part of a close out email, Coulter updated on the work that Protect was doing. Coulter wrote: "We have been working diligently to permanently assign new threats into either blacklist or safe[-]list que. There [are] roughly 225 files that I would like to go over before we take any action. I will send the spreadsheet of these tonight.[576]

Cylance also provided instructions to other entities who were remaining on site at OPM. Coulter wrote:

> If OPM can commit to having all output script results back before Thursday next week this plan will work. I will have 2 of my best guys scheduled to come down Thursday and Friday next week to help in analyzing the results of the *.bat script deployments. We will be done on Friday around [Close of Business] and would like to have a formal meeting with the CyFir & the other team members to close out.[577]

While the situation appeared to be contained, OPM continued to face new and evolving threats. For example, on May 1, 2015, Coulter wrote Wagner and Tonda: ". . . we just saw the very first instance of a prevented Upatre/Dyre Trojan infection (due to setting auto-quarantine). Completely unknown to industry and stopped before it could do any harm."[578]

The Decision to Purchase CylanceProtect

CylanceProtect was the first tool that OPM used after the agency learned its network was compromised, and the tool immediately found malware and set about cleaning OPM's enterprise. This raises a question as to why OPM did not purchase and deploy the tool sooner, in June 2014, when it may have been able to prevent or mitigate the attack, especially given the fact that OPM knew its most sensitive data was being targeted by sophisticated hackers. Documents and testimony show internal agency politics and procurement challenges made it difficult to quickly purchase and deploy security tools.

Political Challenges on the Desktop

On June 12, 2014, less than three months after becoming aware of a significant cyberattack, OPM executed a Cylance product evaluation agreement allowing OPM to test the functionality of both V and Protect for a limited period of time.[579] McClure testified that Cylance's demonstrations typically last 30-60 days, and in "rare exceptions" extend to 90 days.[580] With respect to why OPM was considering their products, McClure stated: "It had been communicated to me through [Cylance staff] that [OPM] had a specific use case or potential problem, that they wanted to test new technology that might be able to help them."[581] However, OPM delayed a decision about acquiring either product for months, even after key officials knew

[576] Coulter Tr., Ex. 14.
[577] *Id.*
[578] Coulter Tr., Ex. 22.
[579] McClure Tr., Ex. 2.
[580] McClure Tr. at 15.
[581] McClure Tr. at 13.

the agency was under attack and despite allocating resources to procure tools to secure OPM's legacy IT environment.[582]

After the March 2014 data breach, OPM's OCIO launched a multi-phased project that included buying security tools to secure the legacy IT environment and create a new IT environment.[583] In June 2014, OPM made a sole-source award to a contractor called Imperatis for this project and CIO Seymour was designed as the OPM official to manage the contract.[584] The estimated cost of the initial project phases was $93 million and $18 million was allocated immediately with the June 2014 award.[585] The first phase of this contract (referred to as the tactical phase) was focused on purchasing security tools for the legacy IT environment to strengthen OPM's legacy systems, but Cylance does not appear to have been considered as part of this contract despite the immediate need for tools like Cylance.

Separately and three months after initially viewing Cylance's products OPM decided to purchase one Cylance product for use in its legacy system on September 27, 2014. The agency opted to purchase V, which is the product limited in scope when compared to Protect, and that did not provide preventative capabilities.[586] This decision was made despite the fact that information security personnel within OPM wanted to acquire Protect, because they recognized its potential to detect threats.[587]

Brendon Saulsbury, a contractor in OPM's IT Security Operations, testified:

> I believe [Cylance Protect] [is] very useful. The fact that they do heuristics-based analysis as opposed to signature-based was beneficial in that they are able to detect our APT malware, which was undetectable at the time by traditional signature-based antivirus tools."[588]

Saulsbury testified he shared that impression of Cylance's products in 2014, long before OPM was in crisis mode, and that he communicated that belief to his managers.[589]

[582] By the end of June 2014, agency officials received US-CERT's final incident report – which made clear that sophisticated attackers were working to acquire information related to the PIPS system. *See* June 2014 OPM Incident Report. OPM was also keenly aware of other deficiencies in its system by this time that it needed to address, such as the OPM Inspector General warning the agency in its fiscal year 2013 FISMA audit that problems in its information systems constituted a "material weakness." *See* Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-13-021, *Federal Information Security Management Act Final Audit FY 2013*, at ii (Nov. 21, 2013) available at: https://www.opm.gov/our-inspector-general/reports/2013/federal-information-security-management-act-audit-fy-2013-4a-ci-00-13-021.pdf..

[583] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 24, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.); *see Infra* Chapter 8 for more on the IT Infrastructure Improvement project and contract.

[584] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015); *Id.* at 000013 (designating Seymour as the contracting officer representative).

[585] *OPM Data Breach: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Office, Offiice of Personnel Mgmt.); Imperatis Letter Contract (June 16, 2014) Attach. 1 at 000006 (Imperatis Production: Sept. 1, 2015).

[586] McClure Tr., Ex. 3.

[587] Wagner Tr. at 91-92.

[588] Saulsbury Tr. at 67-68.

[589] Saulsbury Tr. at 66-68.

Documents and testimony show internal politics contributed to OPM's inability to swiftly purchase the tool that its IT security personnel wanted to acquire, specifically "political challenges on the desktop" at the agency.[590] With respect to the meaning of that term, and why it would have prevented OPM from acquiring Protect in 2014, McClure testified:

> Typically in larger environments, there are other people that own the desktop. So security people don't own the desktop. Security people make recommendations to the desktop teams: You got to do this. You got to do that. You got to install this. You got to install that. And the desktop preparations people usually come from the IT side, the information technology side of the house, versus the security side that usually tries to come outside of the IT to be sort of the watch guard of IT and make sure that what they're doing is secure.
>
> So there's always a firewall, unfortunately, between them, virtually, between the IT guys that try and own the desktop and run the desktop and the security guys who just want the thing to be secure.
>
> Because IT's priorities are around availability predominately, not always confidentiality or integrity, and security is all about confidentiality, integrity, and things like that, so that becomes, unfortunately, a challenge between those organizations. And unless they report separately all the way up to the top, it's always going to favor the folks that own the desktop. The decision-making, the way that they go about trying to find solutions and what they deploy, they control the desktop; they own the desktop, so ultimately they have the last word on what gets installed.[591]

McClure testified:

> [A]necdotally what I have been told was that they had had challenges getting this installed on the endpoint, on the desktop during that initial timeframe in 2014. So because of that, they purchase[d] -- they could only purchase V, which is just this detection product. And I had been told that they were not happy with having to only buy V, that they really wanted to buy PROTECT.[592]

McClure testified these "political challenges"[593] prevented OPM from acquiring Protect, and that had the product been acquired, "It would have prevented this attack."[594]

[590] McClure Tr., Ex. 4.
[591] McClure Tr. at 44-45.
[592] *Id.*
[593] McClure Tr. at 16-17.
[594] McClure Tr. at 16-18.

Counterpoint – Lack of FedRAMP Compliance

OPM's Director of IT Security Operations, Jeff Wagner, testified that political reasons were not why OPM failed to purchase Protect. Wagner stated the primary reason that OPM did not acquire Protect was because "Cylance didn't currently have a FedRAMP-certified cloud."[595]

The Federal Risk Authorization Management Program, or "FedRAMP," is a federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[596] A December 2011 guidance memo issued by the OMB defines the requirements for executive departments and agencies using FedRAMP in the acquisition of cloud services.[597]

Wagner testified that OPM "...had the capability of deploying the Protect tool. We just didn't – because of the FedRAMP issue, **we felt it wasn't necessarily critical at the moment.** It would have been a risk deploying it to a non-fed ramp environment."[598] While Wagner acknowledged that Protect "doesn't necessarily upload sensitive data or PII data or anything of that nature," he testified that a lack of FedRamp authorization was the primary reason for not securing the tool. Wagner testified: "**In a perfect world, we would have deployed it earlier, but because we were trying not to break rules and trying to live within structures, correct, we didn't deploy it.**"[599]

Wagner's assertion that the reason OPM did not buy Cylance tools was because they were not FedRAMP complaint is not supported by the facts. The fact is that OPM ultimately deployed and purchased CylanceProtect without being FedRamp compliant. Protect was not FedRamp compliant when it was first deployed throughout OPM's enterprise on April 17, 2015[600] and it was not FedRamp compliant when it was ultimately purchased in June 30, 2015.[601] **In other words, OPM swiftly broke the rules once its house was already burning down, but not when it was in a position to save it.**

Further, at the same time OPM apparently declined to purchase Protect because it was not FedRAMP compliant, OPM *did purchase V* which was a cloud-based product and not FedRAMP

[595] Wagner Tr. at 91-92. Wagner also said that funding contributed to the decision. However, the funding ultimately obligated to CylanceProtect was a mere fraction of what OPM began immediately spending to build out a new infrastructure. In late October 2015, OPM reported to the Committee that it had spent an estimated $60 million in FY2014 and FY2015 for the new IT infrastructure project. About 80 percent of the funds originated from OPM's revolving fund and the remaining 20 percent from a variety of discretionary and mandatory funds areas. Email from U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Oct. 28, 2015) (on file with Committee).

[596] To learn more about FedRAMP, visit: https://www.fedramp.gov/.

[597] Memorandum from Office of Mgmt and Budget, Exec. Office of the President, to Chief Info. Officers, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 8, 2011), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf.

[598] Wagner Tr. at 112.

[599] Wagner Tr. at 144.

[600] McClure Tr. at 23.

[601] Telephone Interview with Stuart McClure, Chief Exec. Officer, Cylance (Feb. 18, 2016). *See also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015) at CYLANCE _000018 (Cylance Production: Dec. 17, 2015).

compliant at the time. OPM purchased V on September 27, 2014, and the invoice covers Cylance Infinity API, which is the application programming interface for V. Cylance V has both a local- and cloud model.[602] McClure stated: "the V model . . . was cloud-based and local-based."[603]

FedRAMP compliance is an important part of federal agencies' efforts to ensure security and realize efficiencies with cloud-based products. In the case of OPM, however, its compliance efforts were inconsistent when acquiring tools. The agency did not comply with FedRAMP requirements when it purchased Cylance's non-FedRAMP compliant V. Then a mere six months after OPM declined to purchase Protect, OPM asked Cylance for another demonstration of Protect (in the spring of 2015), while the product was still not FedRAMP compliant. On March 20, 2015, OPM executed a clickwrap evaluation agreement that McClure testified is "our internal process for managing somebody that's evaluating our software, so that it doesn't stay in evaluation mode forever. . . So since [OPM] had disengaged on the Protect side the prior year at a certain point, they had come back and said they wanted to retest, so we re-engaged with them through that process."[604] In other words, OPM's interest in Protect did not diminish with time despite the lack of FedRamp compliance. Then after OPM had been breached – OPM deployed Protect – which again was not (at the time) FedRAMP compliant.

OPM ultimately deployed Protect in April 2015, once the agency was in crisis mode, despite its lack of FedRAMP compliance. Director of IT Security Operations Jeff Wagner testified that OPM took this action because "Protect was able to find malware that nothing else could" and he acknowledged that he would have purchased Protect earlier had he been able. He stated:

> Q. So since they didn't have a FedRAMP-certified cloud that would meet all the Federal requirements, we felt it would be less than optimal to go with the PROTECT right away.
>
> A. Cylance was in the process of getting a FedRAMP cloud, and we thought we'd utilize the V as much as we could until they got to that point. I think they're still working to get FedRAMP certified; however, we moved to utilize the PROTECT because it was able to find malware that nothing else could.
>
> Q. Is it fair to say that if it was up to you, you would have gotten PROTECT at the earliest convenience?
>
> A. Absolutely.[605]

The agency purchased Protect on June 30, 2015 when it was still had not been deemed FedRAMP compliant.[606] As of June 2016, Cylance's application is "FedRAMP in Process"[607],

[602] McClure Tr. at 16.
[603] *Id.*
[604] McClure Tr. at 19-20.
[605] Wagner Tr. at 91-92.

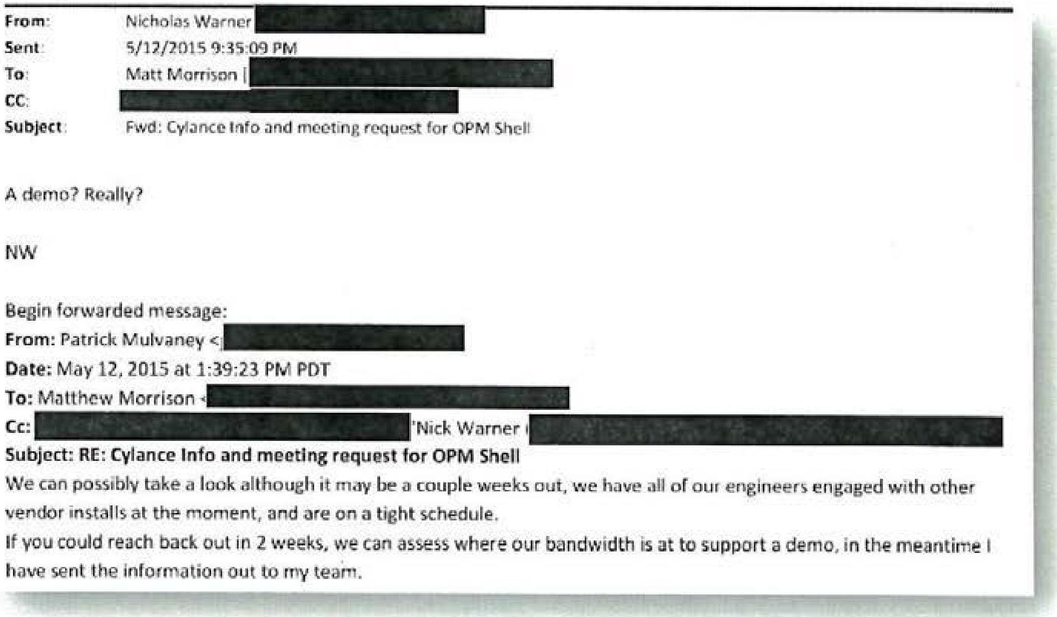
with OMP acting as Cylance's sponsor.[608] It is not known why OPM did not pursue a similar sponsorship path in June 2014.

In sum, Wagner's assertion that OPM did not deploy Cylance's preventative tool – Protect – sooner because it was not FedRAMP compliant is lacking given OPM's actions at the time in buying other non-FedRAMP compliant products.

OPM Purchases Protect After Nearly Losing Access to It

Despite Cylance's significant support to OPM in April through May 2015 following discovery of the attack, OPM was slow to execute payment for services rendered,[609] or execute a purchase agreement for Protect. In addition, OPM and their contractor responsible for building the new IT infrastructure was reticent to consider Cylance tools – despite their proven record during the 2015 incident response period.

OPM's contractor Imperatis, which was responsible for building out the new IT infrastructure, asked Cylance on May 12, 2015 to conduct a demonstration in order to be considered as a security tool for the new IT infrastructure.[610]



From: Nicholas Warner [redacted]
Sent: 5/12/2015 9:35:09 PM
To: Matt Morrison [redacted]
CC: [redacted]
Subject: Fwd: Cylance Info and meeting request for OPM Shell

A demo? Really?

NW

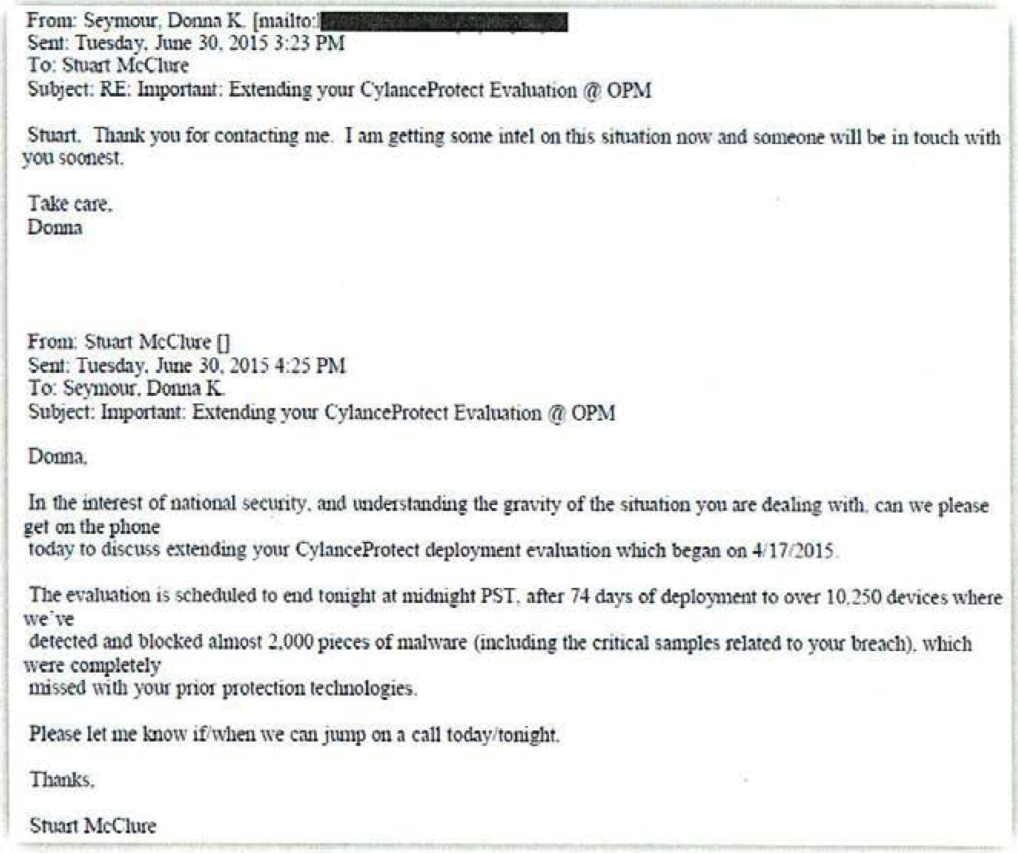
Begin forwarded message:
From: Patrick Mulvaney <[redacted]
Date: May 12, 2015 at 1:39:23 PM PDT
To: Matthew Morrison [redacted]
Cc: [redacted] 'Nick Warner [redacted]
Subject: RE: Cylance Info and meeting request for OPM Shell
We can possibly take a look although it may be a couple weeks out, we have all of our engineers engaged with other vendor installs at the moment, and are on a tight schedule.
If you could reach back out in 2 weeks, we can assess where our bandwidth is at to support a demo, in the meantime I have sent the information out to my team.

[606] McClure Tr., Ex. 1; *see also* Cylance Purchase Order from Assurance Data, Inc. (June 30, 2015) at CYLANCE 000018 (Cylance Production: Dec. 17, 2015).
[607] FedRamp, Cylance, Inc. – CylancePROTECT, https://marketplace.fedramp.gov/index.html#/product/cylanceprotect?sort=productName (Last accessed 090216).
[608] *Id.*
[609] McClure Tr. at 85. (McClure testified that "If I recall, I think it took about 4 or 5 months to get fully paid.").
[610] Coulter Tr., Ex. 23.

The documents show Cylance employees were surprised by the way OPM was handling the procurement process. On June 22, 2015, Cylance CEO McClure emailed a business partner:

> I am having flashbacks to OPM one year ago when they couldn't pull the trigger on Protect because of political challenges on the desktop, so instead only bought V which is detection only. So of course, it didn't prevent the hack they just suffered through, it only notified them after the fact. Then, we installed Protect a year later, in April of this year, and it detected, cleaned and is preventing new attacks every day there. Jeff [Wagner] is kicking himself that he didn't deploy us when 'there wasn't an imminent threat.'[611]

OPM was also slow to ensure they could maintain access to Protect and eventually purchase this tool. On June 30, 2015, Cylance warned CIO Donna Seymour that the agency would lose access to Protect that evening, because the demonstration status was ending and no purchase had been made.



From: Seymour, Donna K. [mailto:[redacted]
Sent: Tuesday, June 30, 2015 3:23 PM
To: Stuart McClure
Subject: RE: Important: Extending your CylanceProtect Evaluation @ OPM

Stuart. Thank you for contacting me. I am getting some intel on this situation now and someone will be in touch with you soonest.

Take care,
Donna

From: Stuart McClure []
Sent: Tuesday, June 30, 2015 4:25 PM
To: Seymour, Donna K.
Subject: Important: Extending your CylanceProtect Evaluation @ OPM

Donna,

In the interest of national security, and understanding the gravity of the situation you are dealing with, can we please get on the phone today to discuss extending your CylanceProtect deployment evaluation which began on 4/17/2015.

The evaluation is scheduled to end tonight at midnight PST, after 74 days of deployment to over 10,250 devices where we've detected and blocked almost 2,000 pieces of malware (including the critical samples related to your breach), which were completely missed with your prior protection technologies.

Please let me know if/when we can jump on a call today/tonight.

Thanks,

Stuart McClure

[611] Email from Stuart McClure, Chief Exec. Officer, Cylance to [redacted] (June 22, 2015, 7:49 a.m.) at CYLANCE_001769 (Cylance Production: Jan. 27, 2016).

McClure wrote to Seymour: "The evaluation is scheduled to end tonight at midnight PST, after 74 days of deployment to over 10,250 devices where we've detected and blocked almost 2,000 pieces of malware (including the critical samples related to your breach), which were completely missed with your prior protection technologies."[612]

Seymour responded: "Thank you for contacting me. I am getting some intel on this situation now and someone will be in touch with you soonest."[613] In July 2015, OPM finally purchased a perpetual license for Protect and access to one year of support and update services that must be renewed on an annual basis (where the initial support services will expire in September 2016). The agency, while now current in payments to the vendor, took four-to-five months to compensate Cylance for its product and work provided.[614]

The significance of the cutting edge preventative technology offered by Cylance in responding to the OPM data breach cannot be overstated. Wagner testified as to why OPM did not find the 2015 attacker, who accessed OPM's system as early as May 7, 2014, prior to the "Big Bang." Wagner cited the fact that OPM did not have a tool like the one Cylance provided. He stated:

> Q. Is it possible that FBI, DHS, and the other folks that were advising you in 2014, that they were unable to detect a latent malware or other parts of that foothold in other directories or portions of the network?
>
> A. Once again, the detection of malware prior to a tool like Cylance is based on what you know. So it's very plausible that there would be instances in which detection would go unnoticed, because you have to know what you're looking for to find it.[615]

Perhaps most importantly, given documents that demonstrate the tool's effectiveness, Cylance would have likely been able to find variants of the malware already on OPM's system in early June 2014 and prevented further compromise. Given that the attackers did not appear to move laterally into the background investigation system until June 23, 2014, if OPM had used CylanceProtect in early June 2014, there is a distinct possibility the exfiltration of data, such as the background investigation data could have potentially prevented and/or the data losses incurred in the fall and early 2015 could have been mitigated.

The Committee obtained documents that show federal agencies are facing a dilemma. On June 18, 2015, the *Washington Post* published a story in which government officials described the challenges that agencies deal with when purchasing cyber technologies.[616] The story stated: "But one challenge was a bureaucracy that made it difficult to buy security tools quickly,

[612] McClure Tr., Ex. 20.
[613] *Id.*
[614] McClure Tr., at 85-86.
[615] Coulter Tr. at 139.
[616] Ellen Nakashima, *Officials: Chinese Had Access to U.S. Security Clearance Data for One Year,* WASH. POST, June 18, 2016, available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year/ /

officials said. 'OPM can't get through government procurement that fast,' said a U.S. official, who was not authorized to speak for the record."[617]

The Committee obtained an internal OPM email that shows OPM's Director of IT Security Operations Jeff Wagner was the anonymous "U.S. official" quoted in the story. The email from Wagner to the *Washington Post* reporter regarding OPM's acquisition of tools following the breach identified in March 2014 stated:

> The following month, in March 2014, the Department of Homeland Security notified OPM of the first hack of the security clearance database. In May that year, the agency did a 'remediation Big Bang,' Wagner said, to try to make improvements to the system. But one challenge was a bureaucracy that made it difficult to buy security tools quickly, he said. 'I can't get through government procurement that fast,' Wagner said. He noted an Office of Inspector General audit suggested 'we were breaking rules by failing to have key systems certified. 'Well, I couldn't go any faster without breaking [procurement] rules.'[618]

The documents and testimony show OPM's IT security personnel identified tools they believed would make the agency's enterprise more secure and failed to purchase and deploy the most effective and cutting edge preventative technology. As the record demonstrates, the Cylance tools later proved invaluable after 74 days of deployment to over 10,000 devices these tools detected almost 2000 pieces of malware on OPM's system and later blocked new threats. Unfortunately, the most effective preventative tool – Protect was not deployed until long after the attackers stole background investigation and fingerprint data and personnel records from OPM's system. The next Chapter describes the assistance another contractor provided to OPM during the 2015 incident response period.

[617] *Id.*

[618] Email from Press Secretary, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (June 18, 2015, 8:01 p.m.), at HOGR 020316-000266-67 (OPM Production: Feb. 16, 2016).

Chapter 5: The CyTech Story

On June 10, 2015, the *Wall Street Journal* reported "four people familiar with the investigation said the [OPM] breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, Inc. which has a network forensics platform called CyFIR."[619] The agency, on the other hand, issued a press release that said the breach was discovered as a result of an "aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks . . . in April 2015, OPM detected a cyber-intrusion affecting its information technology systems and data."[620]

The Committee has investigated the seemingly conflicting statements and as is often the case, the truth is somewhere in between and the story more complicated than it appears. The documents and testimony do not definitively resolve this dispute. They do, however, support the following findings:

1. CyTech, a service disabled veteran-owned small business contractor, participated in several meetings with OPM in early 2015 to discuss the capabilities of their CyTech Forensics and Incident response (CyFIR) tool and to provide a demonstration of their CyFIR tool on April 21, 2015 at OPM headquarters.

2. During CyTech's April 21, 2015 demonstration, CyTech identified or "discovered" malware on the live OPM IT environment related to the incident. There is no evidence showing CyTech was aware at the time of the April 21 demonstration that on April 15 OPM had reported to US-CERT an unknown Secure Sockets Layer (SSL) certificate beaconing to a unknown site (opmsecurity.org), which was an initial indicator of compromise related to the background investigation data breach.[621] The record confirms the agency reported this finding to US-CERT on April 15, 2015.[622] Further, there is no evidence CyTech was aware that OPM (in consultation with Cylance) deployed CylanceV on April 16 and then deployed CylanceProtect on April 17, both of which identified additional key malware samples related to the breach.[623]

3. Beginning on April 22, 2015, CyTech offered and began providing significant incident response and forensic support to OPM related to the 2015 incident. The documents and testimony show OPM and Cylance recognized CyFIR's ability to quickly obtain forensic images. CyTech provided an expert to manage the CyFIR tool and continued to provide onsite support through May 1, 2015. CyTech was not paid for those services.

[619] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.

[620] U.S. Office of Personnel Management, Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015).

[621] AAR Timeline – Unknown SSL Certificate (April 15, 2015), at HOGR020316-1922 (OPM Production: Apr. 29, 2016).

[622] *Id.*; E-mail from [redacted] to CIRT (OPM) (Apr. 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).

[623] *See Supra,* Chapter 4: The Role of Cylance.

4. There is no evidence showing CyTech leaked information about their involvement in responding to the OPM breach to the media. In fact, after the *Wall Street Journal* contacted CyTech on June 9, 2015, (the day before the paper reported CyTech discovered the breach), CyTech immediately contacted OPM. CyTech coordinated with OPM Director of IT Security Operations Jeff Wagner on CyTech's response to the reporter, and CyTech's clarification that they did not advise OPM personnel concerning the incident a year ago. Wagner responded to CyTech's proposed response to the *Wall Street Journal* via email. He wrote: "correct away."[624]

5. Testimony from former OPM Chief Information Officer Donna Seymour to the Committee on June 24, 2015 regarding the CyTech matter is inconsistent with documents and testimony from other witnesses.[625] Seymour testified that OPM purchased CyTech licenses. In fact, OPM did not make any purchases from CyTech. Seymour also testified that CyTech's CyFIR appliance was installed in a quarantine environment for the demonstration. In fact, the CyFIR tool, which runs against programs running in live memory, was running on a live environment when it identified malware on April 22, 2015. Seymour testified that CyTech was given some information regarding indicators of compromise prior to installing the CyFIR appliance on the live IT environment for the demonstration. In fact, CyTech was not given information on indicators of compromise until after they discovered malware on April 22, 2015.

CyTech Is a Small Business Contractor with Significant Cyber Tool Capabilities

CyTech is a service disabled veteran-owned small business. The company was started in 2003 by CEO Ben Cotton. Prior to starting CyTech, Cotton served for more than twenty years in Army Special Forces and specialized in computer forensics. Cotton told the Committee that after he retired, he started CyTech to provide "computer forensics, e-discovery collection, sensitive site exploitation support to the U.S. Government, the intel community, and SOCOM [Special Operations Command], as well as commercial entities."[626] Over the course of his career, Cotton has been qualified as an expert witness on computer forensic matters in a number of matters at the federal and local level.[627] CyTech's clients include military and intelligence entities as well as a major commercial manufacturer.[628]

CyTech offers cyber-related services that include a tool referred to as CyTech Forensics and Incident response (CyFIR). The CyFIR tool was released for public sale in 2014.[629] Cotton described CyFIR in his testimony to the Committee. He stated: "fundamental to CyFIR is a concept we call speed to resolution. . . . which is the ability to identify malware or breach

[624] Cotton Tr., Ex. 9.
[625] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, Office of Pers. Mgmt.).
[626] Cotton Tr. at 6.
[627] Cotton Tr. at 6-7.
[628] Cotton Tr. at 7.
[629] Cotton Tr. at 8.

conditions inside of a network, to investigate those anomalies, to isolate them, and to remediate them."[630] He also stated:

> The value add to CyFIR is the speed that we can perform these discovery, investigative and remediation functions . . . specifically in the incident response and the network forensics realms. We have the ability to simultaneously conduct searches and do assessments on every single end point inside of an environment. EnCase [a competing tool], due to its technology limitations, can only search a limited subset of that, and the number of . . . end points that it can search is dependent upon basically the network infrastructure and the ability for it to pull that data from the end points back to the investigative console. . . . our search results . . . can come back to us in as little as 45 seconds, where with the other competitive tools, which EnCase is one of them, that typically takes days or weeks to get that information back.[631]

Cotton also stated that CyFIR is "designed to run in a live environment" and it is "not a dead drive forensics tool."[632] He testified about the challenges of modern cyber threats. He stated: "we need to eliminate the time constraints that are imposed by using dead drive forensics tools to investigate incident response. And so we've done that [with CyFIR]. We operate strictly on live systems."[633]

In 2014, CyTech began promoting the CyFIR tool through outreach to various partners and an exhibition at the 2014 RSA Security LLC conference.[634] This outreach ultimately led to the demonstration of the CyFIR tool at OPM on April 21, 2015.

CyTech Was Invited to Conduct a Demo at OPM

In response to the OPM cyber incident first identified in March 2014 and after subsequently identifying serious vulnerabilities in the OPM network, OPM initiated the IT Infrastructure Improvement project.[635] In June 2014, OPM awarded a sole source contract to Imperatis to serve as prime contractor for the project.[636] As part of this contract, the prime contractor was directed to identify, evaluate and recommend security tools to secure OPM's legacy IT environment and design and build a secure new IT environment. CyTech was among the tools that Imperatis and OPM considered as part of this effort.[637]

[630] Cotton Tr. at 8.

[631] Cotton Tr. at 9.

[632] Cotton Tr. at 10.

[633] *Id.*

[634] Cotton Tr. at 8; *CyFIR*, RSA CONFERENCE, http://www.rsaconference.com/events/us14/exhibitors-sponsors/exhibitor-list/1139/cyfir (last visited April 10, 2016) (list of products available at 2014 RSA Conference).

[635] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[636] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015). A sole source contract is a contract that was awarded without being subject to the competitive bidding process. *See Infra*, Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach.

[637] Security Tool/Vendor Demonstrations, Attach. 11 at 001441-42 (Imperatis Production: Sept. 1, 2015).

Prior to the April 21, 2015 CyFIR Demonstration at OPM

Documents and testimony show OPM had interest in the CyFIR tool beginning in February 2015, and meetings were scheduled to learn more about the tool.[638] Imperatis coordinated two meetings for OPM at CyTech headquarters to discuss the CyFIR tool on March 27, 2015 and April 2, 2015.[639]

At the March 27 meeting, according to Cotton, Wagner's reaction to the CyFIR tool was "very positive" and OPM requested another meeting to include additional OPM staff.[640] At the April 2 meeting, according to Cotton, Wagner's reaction was again "extremely positive" and OPM told CyTech they wanted CyTech to bring the CyFIR appliance to OPM for a demonstration to "let them kick the tires . . . on CyFIR inside their environment."[641]

Wagner testified that "CyTech was a potential replacement of our current EnCase capability, because they were indicating that their client tool was able to take the forensic image remotely and then transmit the image file back instead of a piece of the image file at a time."[642]

After these two meetings, the onsite CyFIR demonstration was scheduled for April 21, 2015 at OPM headquarters.

The April 21, 2015 – April 22, 2015 CyFIR Demonstration at OPM

In preparation for the demonstration at OPM headquarters, CyTech ordered and configured a CyFIR appliance.[643] Then, on April 20, 2015, Imperatis employee [redacted] informed Wagner that the CyFIR tool was ready for the OPM team to "give it a run through" and that Cotton was available to be on site with demo licenses for about fifty agents.[644] On the morning of April 21, 2015, Cotton arrived at OPM headquarters for the demonstration.[645]

[638] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Matthew Morrison, Assurance Data, Inc. (Feb. 23, 2015, 1:51 p.m.), at HOGR020316-000292 (OPM Production: Feb. 16, 2016).

[639] Security Tool/Vendor Demonstrations, Attach. 11 at 001441-42 (Imperatis Production: Sept. 1, 2015); Cotton Tr., Ex. 1; Email from [redacted] Imperatis, to Jonathon Tonda, Contractor, U.S. Office of Pers. Mgmt.(Mar. 30, 2015, 1:51 p.m.), at HOGR020316-000298 (OPM Production: Feb. 16, 2016); Imperatis Weekly Report (Mar. 30, 2015 to Apr. 3, 2015), Attach. 6 at 000704 (Imperatis Production: Sept. 1, 2015).

[640] Cotton Tr. at 12-13; Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Sept. 1, 2015) (stating after the March 27, 2015 meeting "Wagner requested an additional follow up meeting for several members of his staff to be briefed on CyFIR.") (on file with the Committee).

[641] Cotton Tr. at 13; Apr. 2, 2015 Meeting Acceptance by Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Mar. 31, 2015), at HOGR020316-000301 (OPM Production: Feb. 16, 2016); Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Sept. 1, 2015) (stating OPM interested in the CyFIR tool and a subsequent meeting was arranged for an onsite CyFIR demonstration) (on file with the Committee).

[642] Wagner Tr. at 97-98.

[643] Cotton Tr., Ex. 2 (CyFIR Appliance and Configuration Invoice for $7943 (Apr. 3, 2015)).

[644] Email from [redacted] Imperatis to Jeff Wagner, Dir. Info. Tech. Sec. Operations and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 20, 2015, 4:22 p.m.), at HOGR0909-000007 (OPM Production: Oct. 28, 2015).

[645] OPM Visitor Log, Washington, D.C. (Apr. 21, 2015), at HOGR020316-000522 (OPM Production: Feb. 16, 2016). On September 28, 2015, OPM produced a highly redacted version of the above cited visitor log in response to a July 24, 2015 request. The initial version was so heavily redacted that no names were provided, including

Wagner testified that he forgot the demonstration had been scheduled, but he decided to go forward with the demonstration "because we had something interesting going on, it would be interesting to see what the tool could do."[646] The decision to conduct a demonstration in the midst of an incident response effort is interesting given the severity of the incident.

During a demonstration of the CyFIR tool, CyTech usually provides a license with a limited number of agents to be deployed. For purposes of the OPM demonstration that began on April 21, Cotton testified: "we had a very limited license on the number of agents."[647] Cotton stated CyTech arranged for twenty agents to be pushed out by OPM for the demonstration.[648]

Cotton stated that OPM did not give him any specific instructions or configurations prior to the April 21, 2015 demonstration, nor was he given indicators of compromise to look for when the CyFIR appliance was installed.[649] The agency later claimed that indicators of compromise were given to CyTech prior to installation.[650] The documents and testimony show, however, that CyTech was recruited to provide assistance to OPM and given indicators of compromise only after it had successfully identified malware in the live environment.

With respect to where the appliance was installed on April 21, 2015, Cotton testified: "we left it up to OPM as to what computers or what environment we would be put into."[651] In other words, it was up to OPM to decide where to deploy the CyFIR agents.

Cotton stated he spent a significant amount of time waiting for permissions and access to IT facilities on April 21. By the time the CyFIR appliance was installed it was late in the day and Cotton's escort "had to catch a bus" so the demonstration had to continue the next day.[652] Before he left, Cotton activated the CyFIR tool's cyber threat assessment function, which takes a snapshot of all the computers where CyFIR is installed and then compares the snapshot against "known good, known bad, and unknown processes."[653]

There is no evidence that shows CyTech received specific information about where on the OPM network CyFIR was deployed. Documents and testimony do show, however, that on April 21, 2015, the CyFIR tool was deployed to a live production environment where it identified malware when results of the demonstration were examined the following day. Wagner

Cotton's. After multiple requests and almost seven months after the initial request, the Committee finally obtained a readable version of the OPM visitor log in February 2016.

[646] Wagner Tr. at 99.

[647] Cotton Tr. at 16.

[648] *Id.*

[649] Cotton Tr. at 14, 16.

[650] Notably, OPM appears to assert that an April 23, 2015 email exchange supports the statement that OPM provided the indicators of compromise to CyTech to find the malware prior to the April 21/22 CyFIR demonstration. *See* Email from Jonathon Tonda, Contractor, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 15, 2015, 2:35 p.m.) with Attach. Email from Brendan Saulsbury Senior Cyber Security Engineer, SRA, to [redacted] Imperatis (Apr. 23, 2015, 12:47 p.m.), at HOGR020316-000254 (OPM Production: Feb. 16, 2016).

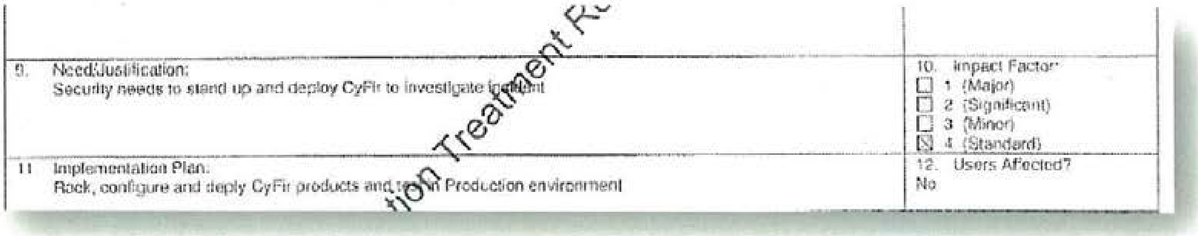
[651] Cotton Tr. at 16.

[652] *Id.*

[653] Cotton Tr. at 16-17.

testified the tool was deployed in a live production environment and that the CyFIR tool did identify malware.[654]

In fact, OPM's Production Change Request Form for the April 21, 2015 CyFIR demonstration was signed by Wagner that day. It states that the Change Request was "Urgent"; that the "Need/Justification" for deploying CyFIR was because "Security needs to stand up and deploy CyFIR to investigate incident"; and that the "Implementation Plan" was to "Rack, configure and deploy CyFIR products and test in production environment."[655]



9. Need/Justification: Security needs to stand up and deploy CyFir to investigate incident	10. Impact Factor: ☐ 1 (Major) ☐ 2 (Significant) ☐ 3 (Minor) ☒ 4 (Standard)
11 Implementation Plan: Rack, configure and deply CyFir products and test in Production environment	12. Users Affected? No

The Change Request Form lists five areas where the CyFIR tool was to be deployed on April 21, 2015—all five were live production servers. The next day, on April 22, 2015, Cotton returned to OPM to continue the demonstration.[656] Upon arrival, Cotton accessed the CyFIR threat assessment screen and found the tool had identified known malware as well as "a subset of unknown processes . . . masquerading as McAfee executables" according to the CyFIR categorization system.[657]

Cotton testified he put the malware CyFIR found on a thumb-drive and gave it to [redacted] [redacted] who worked for Imperatis and was escorting Cotton at OPM.[658] Cotton stated that he believed [redacted] provided the information to OPM IT Security Operations. Wagner testified "CyFIR was able to find malware within the [OPM IT] environment" and was deployed in a live environment.[659]

US-CERT confirmed Cotton's assessment that CyFIR found malware on a key server. In fact, four of the five servers that CyFIR was loaded onto April 21, 2015 were implicated in the personnel and background investigation data breach.[660] While CyTech's CEO was not told

[654] Wagner Tr. at 102-103. The OPM Director of IT Security Operations added that CyFIR "did not find specifically anything that we hadn't already found." *Id.* at 16.
[655] OPM Production Change Request Form for Apr. 21, 2015 CyFIR Demonstration, at HOGR0909-000090-91 (OPM Production: Oct. 28, 2015).
[656] OPM Visitor Log, Washington, D.C. (Apr. 22, 2015), at HOGR02316-000525 (OPM Production: Feb. 16, 2016).
[657] Cotton Tr. at 19.
[658] *Id.* In February 2016, the Committee inquired with Imperatis, [redacted] employer, about the status of this thumb drive, but the thumb drive was not located. Notably, Imperatis stated Mr. Cotton did not provide a thumb drive to [redacted] with incident response data, but [redacted] was told by another CyTech employee such a thumb drive was given to the FBI. Imperatis Memo to Majority Staff (Feb. 3, 2016), on file with staff.
[659] Wagner Tr. at 102-103. The Director [Wagner] added that "it did not find specifically anything that we hadn't already found." *Id.* at 102.
[660] OPM Production Change Request Form for Apr. 21, 2015 CyFIR Demonstration, at HOGR0909-000090 to 91 (OPM Production: Oct. 28, 2015).

going into the demonstration that all of the malware Cylance identified on April 21, 2015 had been previously identified with the Cylance tools, it is indisputable that CyFIR did identify malware on four of the five servers it was deployed to during the April 21, 2015 product demonstration. The documents show:

- CyFIR was installed on server [redacted] on April 21, 2015.[661] On this server [redacted] which is believed to be a workstation, Cylance found the [redacted] malware on April 21, 2015 and discussed it via email at 12:51 a.m.[662] [redacted] was a [redacted] Hikit that pointed to the malicious domain [redacted] CyFIR identified malware on this server April 21, 2015.[663] This information was provided to US-CERT and it subsequently appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[664]

- CyFIR was installed on server [redacted] on April 21, 2015.[665] On this server [redacted] CylanceProtect also found the Trojan [redacted] on April 21, 2015 and discussed it via email at 12:51 a.m.[666] [redacted] was a Hikit RAT (Remote Administration Tool) and the DLL (Dynamic Link Libraries) would attempt to read a configuration file in the same folder it was executed.[667] CyTech identified malware on this server. This information was provided to US-CERT, and it subsequently appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[668]

- CyFIR was installed on [redacted]—a key Microsoft database server. It was on this server that CylanceV initially identified the malicious executables on April 16, 2015 that US-CERT would affirm as a malicious PlugX package on April 17, 2015.[669] CyTech identified malware on this server.

- CyFIR was installed on server [redacted] on April 21, 2015.[670] CylanceProtect would identify a RAR SFX2 folder on this server that was created in a

[661] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[662] Coulter Tr., Ex. 7.

[663] *Id.*

[664] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[665] *Id.*

[666] Coulter Tr., Ex. 7. *See also* Coulter Tr., Ex. 3.

[667] U.S. Dep't of Homeland Security/US-CERT, Malware Analysis Report-460357-A (April 24, 2015) at 000190 (US-CERT Production: Dec. 11, 2015).

[668] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[669] Email from [redacted] to Brendan Saulsbury, Senior Cyber Sec. Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[670] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

"McAfeeSVC" folder in a directory—a folder that was part of a malicious PlugX package. This RAR SFX2 would also be found on its aforementioned duplicate server [redacted] CyTech identified malware on this server.

- CyFIR was installed on sever [redacted] on April 21, 2015. The documents obtained by the Committee do not make reference to this server.

According to Cotton, around lunchtime on April 22, 2015, there was a brief meeting between Wagner and [redacted] Cotton's escort.). Wagner asked, "they found it?"[671] [redacted] nodded.[672] Cotton testified that Wagner requested "an emergency purchase order for CyFIR inside of the legacy [IT environment]" for a license with 15,000 agents and several CyFIR appliances as well as 1,000 hours for personnel support.[673]

Cotton testified that on April 22, 2015, he offered incident response and forensic assistance to OPM, and OPM accepted.[674] Cotton subsequently met briefly with US-CERT and the FBI to describe CyFIR findings and said it was his understanding that "OPM had turned over the malware that we had imaged that morning to them [US-CERT]."[675] Late on April 22, 2015, Cylance began working with CyTech and requested that CyTech pull system files to support forensic analysis.[676] Cotton testified that he contacted CyTech's senior incident response expert, Juan Bonilla, who was not part of the original demonstration, and directed him "to fly in as early as he could to assist with the incident response."[677]

The documents and testimony show OPM quickly escalated the use of CyFIR within the agency's environment after CyFIR successfully identified malware. For example, on April 22, 2015, at 3:53 p.m., CyFIR was loaded on server [redacted][678] This server provided access to the PIPS mainframe.

On April 23, 2015, CyFIR was loaded on its duplicate server [redacted].[679] CyFIR was put on servers [redacted] and [redacted] on April 17, 2015, and the images CyFIR extracted from these two servers were supplied to US-CERT appeared in US-CERT's May 4, 2015 Preliminary Digital Media Analysis Report.[680] These

[671] Cotton Tr. at 20.
[672] *Id.*
[673] *Id.*
[674] Cotton Tr. at 39-41.
[675] Cotton Tr. at 27; CyTech Demonstration/Results Participants, at HOGR0724-000322 (OPM Production: Sept. 25, 2015) (showing CyTech demonstration/ results participants included FBI, US-CERT, OPM, OPM contractors, Imperatis, and Cytech).
[676] Email from Chris Coulter, Managing Dir., Cylance to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 22, 2015, 7:01 p.m.), at HOGR020316-000008 (OPM Production: Feb. 16, 2016).
[677] Cotton Tr. at 25. Cotton noted that CyTech's expert, Bonilla, as a senior member of the CyTech team, is typically billed at between $450 and $350 an hour. *Id.*
[678] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[679] *Id.*.
[680] *Id.*.

servers [redacted] are also critical because it provided access to the PIPS mainframe.

US-CERT's reports show CyFIR was placed on an additional key server and its duplicate [redacted] on April 23 at 2:27 p.m.[681] This sever is a critical jump box that provided access to the portion of OPM's environment segments where the PIPS mainframe resides.[682] While Cylance was installed on these servers at 6:21 p.m. on April 17, 2015, CyFIR was assisting with forensic work.

Documents show OPM, after reviewing the results of the CyTech demonstration, deployed CyFIR to key servers that gave access to critical parts of OPM's environment, including one of the most important and sensitive servers that gave access to the PIPS mainframe, where sensitive background investigation data was stored. This suggests OPM believed CyTech could assist the agency in the incident response situation.

By April 24, 2015, and in response to Wagner's verbal request for services, CyTech submitted a quote to OPM through Imperatis.[683] CyTech quoted $818,000 for a perpetual license with 15,000 agents.[684] The documents show there was a serious effort to finalize OPM's verbal request for services and that the participants in the April 22 meeting understood OPM's intent. Sometime the week of April 27, Imperatis reported "coordinating equipment installation and configuration with security vendors" including "working to finalize BOM [bill of materials]" for CyFIR.[685] In an interview with the Committee, Wagner testified that he did not say OPM would buy CyFIR, but acknowledged that he likely asked for a quote.[686] CyTech relied on the request for services that exceeded the scope of a typical demonstration and expanded the services it provided to OPM during the 2015 incident response period. Consequently, on April 22, 2015, CyTech provided a license to OPM for 1,000 endpoints that expired on June 30, 2015.[687]

Cotton testified that CyTech provided incident response and forensic assistance to OPM out of a sense of duty and with the expectation that there would be a contractual arrangement put into place.[688] Cotton stated there was a promise of a contract, but execution was delayed repeatedly.[689] With respect to why CyTech provided these services without a contract in place, Cotton testified:

[681] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

[682] Saulsbury Tr. At 75-76.

[683] Cotton Tr., Ex. 3,4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).

[684] *Id.*

[685] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach 6 at 000758 (Imperatis Production: Sept. 1, 2015).

[686] Wagner Tr. at 104.

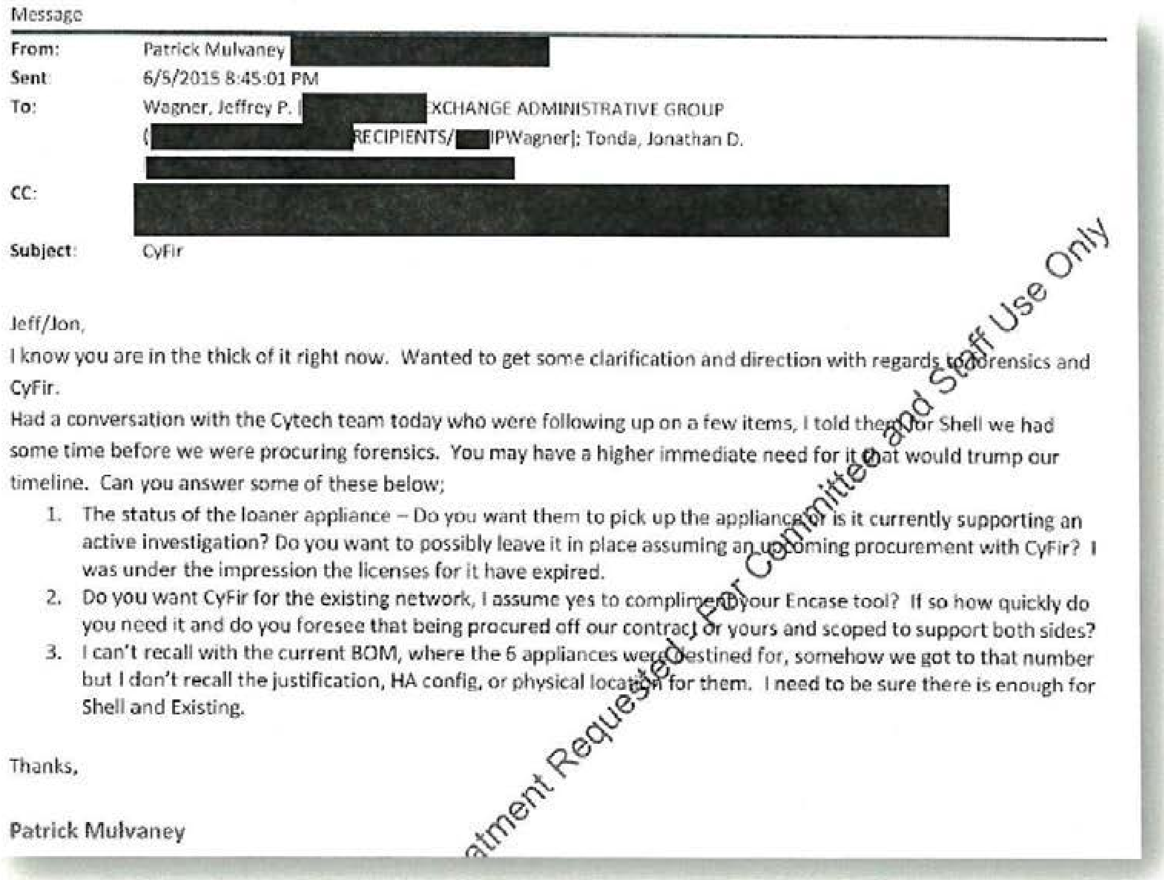
[687] Cotton Tr. at 25; *see also* Email from Ben Cotton, Chief Exec. Officer, CyTech, to H. Comm. on Oversight & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).

[688] Cotton Tr. at 41.

[689] Cotton Tr. at 40.

> Typically, there is [a contract in place]. It's also atypical that we are doing a demonstration and we find live malware on the end points of a government agency that, quite frankly, controls my security clearance. I knew immediately, once it was determined that this was malware, what the implications could be for the country. So, you know, maybe I'm a bad businessman, maybe I'm too much of a patriot at this point, but I didn't want to leave them in the lurch and I didn't want to let this breach go without a capability that would help minimize this to OPM.[690]

Just days before OPM denied CyTech's role in the response to the media, OPM personnel and Imperatis shared internally the clear expectation that OPM would be compensating CyTech for CyFIR and incident response and forensic support based on the conversations CyTech had with OPM in mid-April 2015. On June 5, 2015, Imperatis inquired about the status of the CyTech quote. An Imperatis employee asked an OPM official: "do you want CyFIR for the existing network, I assume yes to compliment your Encase tool?"[691]



Message

From: Patrick Mulvaney [redacted]
Sent: 6/5/2015 8:45:01 PM
To: Wagner, Jeffrey P. [redacted]XCHANGE ADMINISTRATIVE GROUP
([redacted]RECIPIENTS/[redacted]IPWagner]; Tonda, Jonathan D.
[redacted]
CC: [redacted]
Subject: CyFir

Jeff/Jon,
I know you are in the thick of it right now. Wanted to get some clarification and direction with regards to forensics and CyFir.
Had a conversation with the Cytech team today who were following up on a few items, I told them for Shell we had some time before we were procuring forensics. You may have a higher immediate need for it that would trump our timeline. Can you answer some of these below;

1. The status of the loaner appliance – Do you want them to pick up the appliance or is it currently supporting an active investigation? Do you want to possibly leave it in place assuming an upcoming procurement with CyFir? I was under the impression the licenses for it have expired.
2. Do you want CyFir for the existing network, I assume yes to compliment your Encase tool? If so how quickly do you need it and do you foresee that being procured off our contract or yours and scoped to support both sides?
3. I can't recall with the current BOM, where the 6 appliances were destined for, somehow we got to that number but I don't recall the justification, HA config, or physical location for them. I need to be sure there is enough for Shell and Existing.

Thanks,

Patrick Mulvaney

[690] Cotton Tr. at 40-41.
[691] Email from Patrick Mulvaney, Imperatis to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (June 5, 2015, 8:45 p.m.), at HOGR0909-000046 (OPM Production: Oct. 28, 2015).

The CyTech Demo Turned into Incident Response and Forensic Support

In mid-April through May 2015, significant incident response and forensic support activity was underway at OPM. Documents and testimony show CyTech was part of that effort. Other contractors that were onsite confirmed CyTech's role. Cylance was one such contractor. A Cylance official testified CyTech was providing assistance onsite with a tool "that can make it easier to obtain evidence" and that "having that [tool] actually was useful. It sped up the initial triage process of trying to obtain critical forensic artifacts."[692]

Another contractor who staffed the OPM IT Security Operations group said, "…OPM made a decision to have the CyFIR product…assist with gathering forensic images, of some of the servers, that US-CERT requested the image."[693] Yet another OPM contractor, Imperatis, reported that "CyFIR (forensics tool) [was] installed in legacy environment through operational testing" and "has proven to be extremely beneficial in the reduction of man hours required with an active security issue."[694]

CyTech Provided Onsite Incident Response and Forensic Support From April 23 to May 1, 2015

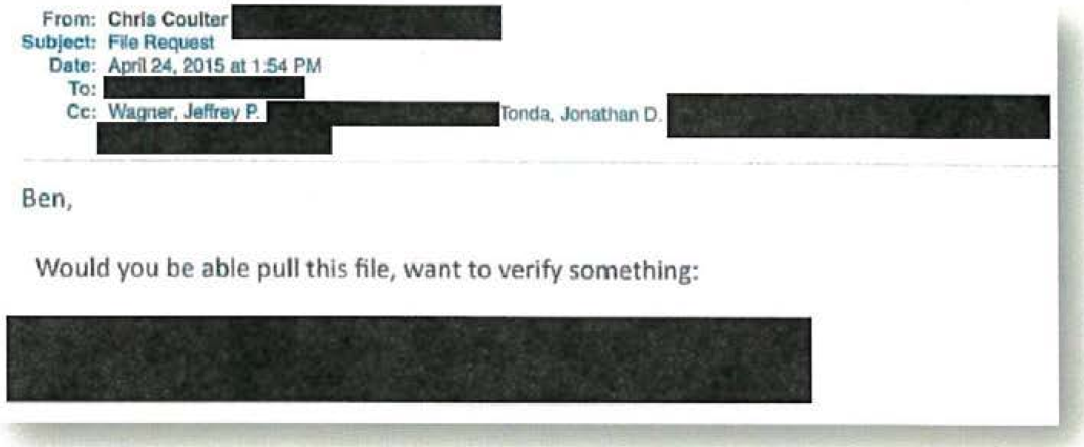
The Committee obtained documents and testimony that show CyTech provided specific incident response and forensic support activities to OPM. On April 23, 2015, after the CyFIR demonstration, Cotton returned to OPM to provide assistance.[695] Cotton also brought a CyTech expert, Juan Bonilla, whose services are billed at $350 to $450 an hour, to assist OPM with the CyFIR tool.[696] Bonilla remained onsite at OPM through May 1, 2015.[697] Documents show that it was an incident response and forensic support environment at that time. The FBI and US-CERT were also onsite on April 23, 2015 and returned for several days thereafter.[698]

In testimony to the Committee and in public statements, OPM officials downplayed CyTech's role in the incident response and forensic support operation in April-May 2015. For example, Wagner testified Bonilla "wasn't really part of the investigation."[699] In an email from April 28, 2015, however, Wagner notified OPM IT administrators that Bonilla would be

[692] Coulter Tr. at 68-69.
[693] Saulsbury Tr. at 84.
[694] Imperatis Weekly Report (Apr. 20, 2015-Apr. 24, 2015), Attach. 6 at 000743 (Imperatis Production: Sept. 1, 2015).
[695] OPM Visitor Log Washington, D.C. (Apr. 23, 2015) at HOGR020316-000530 (OPM Production: Feb. 16, 2016).
[696] *Id.*; Cotton Tr. at 25.
[697] Cotton Tr. at 26; Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Jonathan Tonda, Contractor and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (May 1, 2015, 12:43 p.m.), at HOGR020316-000067 (OPM Production: Feb. 16, 2016) (showing Bonilla coordinating collection of images with OPM prior to May 1 departure); Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 1, 2015, 5:09 p.m.), at HOGR020316-000068 (OPM Production: Feb. 16, 2016) (indicating Bonilla left CyFIR credentials for OPM's use).
[698] OPM Visitor Log, Washington, D.C. (Apr. 23, 2015), at HOGR020316-000529-30 (OPM Production: Feb. 16, 2016).
[699] Wagner Tr. at 101.

"assisting with an investigation over the next two weeks" and asked what needed to be done to obtain system access for him.[700] Wagner also testified Bonilla and Coulter worked together during the incident response. Wagner stated: "we threw everybody into a giant room, and Juan [Bonilla] was the CyTech engineer, much like Coulter was the Cylance engineer. . . ."[701] Clearly, Cylance had a significant role in incident response and the comparison between CyTech and Cylance personnel onsite suggests at the very least CyTech played a supporting role in incident response that OPM has not publicly acknowledged.

In terms of other specific CyTech activities, Cotton testified CyTech was initially asked to image all the random access memory from approximately fifty computers, image the hard drives for those computers, and pull event logs for OPM.[702] CyTech also worked with Cylance to fulfill their requests for files. For example, on April 24, 2015, Cylance asked CyTech to pull a ".bat" file.[703] Cotton testified that ".bat" files "are commonly used as part of a breach to automate the infestation or the installation of malware."[704]



From: Chris Coulter [redacted]
Subject: File Request
Date: April 24, 2015 at 1:54 PM
To: [redacted]
Cc: Wagner, Jeffrey P. [redacted] Tonda, Jonathan D. [redacted]

Ben,

Would you be able pull this file, want to verify something:

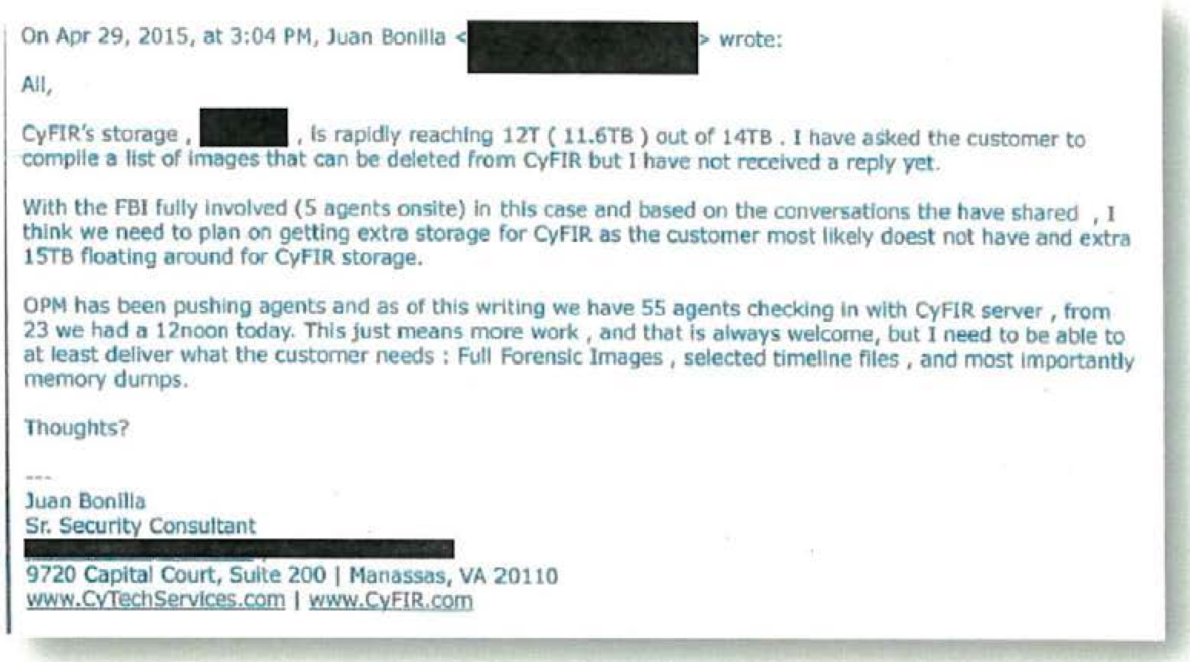
[redacted]

Bonilla worked with OPM to deploy CyFIR and coordinated with OPM staff to address connectivity issues.[705] Documents show that as of April 28, 2015, Wagner prioritized CyFIR deployment to at least thirty-eight servers.[706]

Documents show CyTech collected thousands of images in its forensic support role. Indeed, the documents show the CyFIR appliance was literally running out of memory space to retain all of these images. On April 29, 2015, Bonilla requested information from OPM about a

[700] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., toJames Anderson, U.S. Office of Pers. Mgmt. (Apr. 28, 2015, 5:43 p.m.) at HOGR020316-000707 (OPM Production: Mar. 16, 2016).
[701] Wagner Tr. at 100.
[702] Cotton Tr. at 27-28.
[703] Email from Chris Coulter, Managing Dir., Cylance to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).
[704] Cotton Tr. at 29.
[705] Emails between Juan Bonilla, Senior Sec. Consultant, CyTech, and Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 27, 2015) at HOGR020316-000026-28 (OPM Production: Feb. 16, 2016).
[706] Message from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 28, 2015, 9:04 p.m.) at HOGR020316-000333 (OPM Production: Feb. 16, 2016).

list of images that needed to be retained because the CyFIR appliance only had fourteen terabytes of storage space and was quickly nearing capacity.[707] Cotton testified that OPM asked CyTech "to collect all this information and we were running out of storage for that."[708]



On Apr 29, 2015, at 3:04 PM, Juan Bonilla <[redacted]> wrote:

All,

CyFIR's storage , [redacted] , is rapidly reaching 12T (11.6TB) out of 14TB . I have asked the customer to compile a list of images that can be deleted from CyFIR but I have not received a reply yet.

With the FBI fully involved (5 agents onsite) in this case and based on the conversations the have shared , I think we need to plan on getting extra storage for CyFIR as the customer most likely doest not have and extra 15TB floating around for CyFIR storage.

OPM has been pushing agents and as of this writing we have 55 agents checking in with CyFIR server , from 23 we had a 12noon today. This just means more work , and that is always welcome, but I need to be able to at least deliver what the customer needs : Full Forensic Images , selected timeline files , and most importantly memory dumps.

Thoughts?

Juan Bonilla
Sr. Security Consultant
[redacted]
9720 Capital Court, Suite 200 | Manassas, VA 20110
www.CyTechServices.com | www.CyFIR.com

It is worth noting, during what would turned out to be most damaging data breach in the history of the federal government, OPM was making decisions about what forensic evidence to retain without it appears consulting the OIG or counsel in a meaningful way.

In late April 2015, CyTech and Cylance continued to assist OPM. On April 29, 2015, Cylance and CyTech updated OPM on the status of Cylance's analysis efforts. Coulter testified that there were three teams working on incident response with OPM: Cylance, CyFIR, and law enforcement. With respect to CyTech's role, Coulter stated "as Cylance through CylanceProtect was identifying new instances of malware that were related, we would then request CyFIR to install an agent on that machine to then collect the data for further analysis."[709] An April 29, 2015 email from Coulter stated that CyFIR would install "agents on the scoped hosts and collect data for the other team" and suggested a "formal meeting with the CyFIR & other team members to close out."[710]

[707] Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 29, 2015, 5:26 p.m.) at HOGR020316-000043 (OPM Production: Feb. 16, 2016).
[708] Cotton Tr. at 31; Cotton Ex. 6 (showing internal CyTech discussion about storage options and how such costs may be covered under a contract); Text Message from Jeffrey Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 30, 2015) at HOGR020316-000347(OPM Production: Feb. 16, 2016) (showing internal OPM discussion on options for CyFIR to dump images).
[709] Coulter Tr. at 71.
[710] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Apr. 29, 2015, 4:40 p.m.) at HOGR020316-000337 (OPM Production: Feb. 16, 2016).

In sum, CyTech was onsite at OPM from April 21 to May 1, 2015. During that time, CyTech identified malware and provided incident response and forensic support to OPM that exceeded the scope of the product demonstration that began on April 21.

CyFIR Was Deployed on the OPM Network beginning in April 2015 and Remained on OPM's Network through August 2015

Wagner testified that "once Bonilla left the site, we never utilized CyTech's product again." [711] Documents suggest otherwise. After Bonilla left OPM on May 1, 2015, CyTech continued to provide assistance on an as needed basis. On May 8, 2015, Bonilla emailed Wagner to follow up on the work he did the week before and offered to provide additional assistance with the CyFIR tool.[712]

The documents show OPM continued to use the CyFIR tool from May 2015 through early June. For example, on May 7, 2015, Cylance requested CyFIR be deployed to a particular OPM host.[713] On May 28, 2015, an OPM contractor stated that CyFIR had collected images from a key production server.[714] On June 1, 2015, an OPM contractor wrote: "all other security agents are currently running, Cylan[c]e, CyFIR, Forescout."[715]

Documents show the forensic capabilities of the CyFIR tool were a continuing topic of discussion. For example, Imperatis, the OPM contractor who introduced CyTech to OPM, described a May 15, 2015 "forensics capabilities meeting with CyFIR."[716] Documents show there were continuing interactions with CyTech and use of the CyFIR tool through June 2015.[717]

Wagner minimized the scope of the CyFIR deployment in his testimony to the Committee. He stated: "we only deployed their CyFIR client to a select number of machines."[718] Documents show, however, CyFIR's deployment was fairly extensive. The Committee obtained documents that show the CyFIR tool was tested on more than sixty different servers, including key servers connected to the personnel records and background investigation data that was exfiltrated.[719]

[711] Wagner Tr. at 105.

[712] Email from Juan Bonilla, Senior Sec. Consultant, CyTech to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (May 8, 2015, 5:49 p.m.) at HOGR020316-000071 (OPM Production: Feb. 16, 2016).

[713] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 7, 2015, 3:56 p.m.) at HOGRO020316-000351 (OPM Production: Feb. 16, 2016).

[714] Email from Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt., to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (May 28, 2015, 1:43 p.m.) at HOGR020316-000360 (OPM Production: Feb. 16, 2015).

[715] Email from [redacted] Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees [redacted]] (June 1, 2015, 3:28 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016).

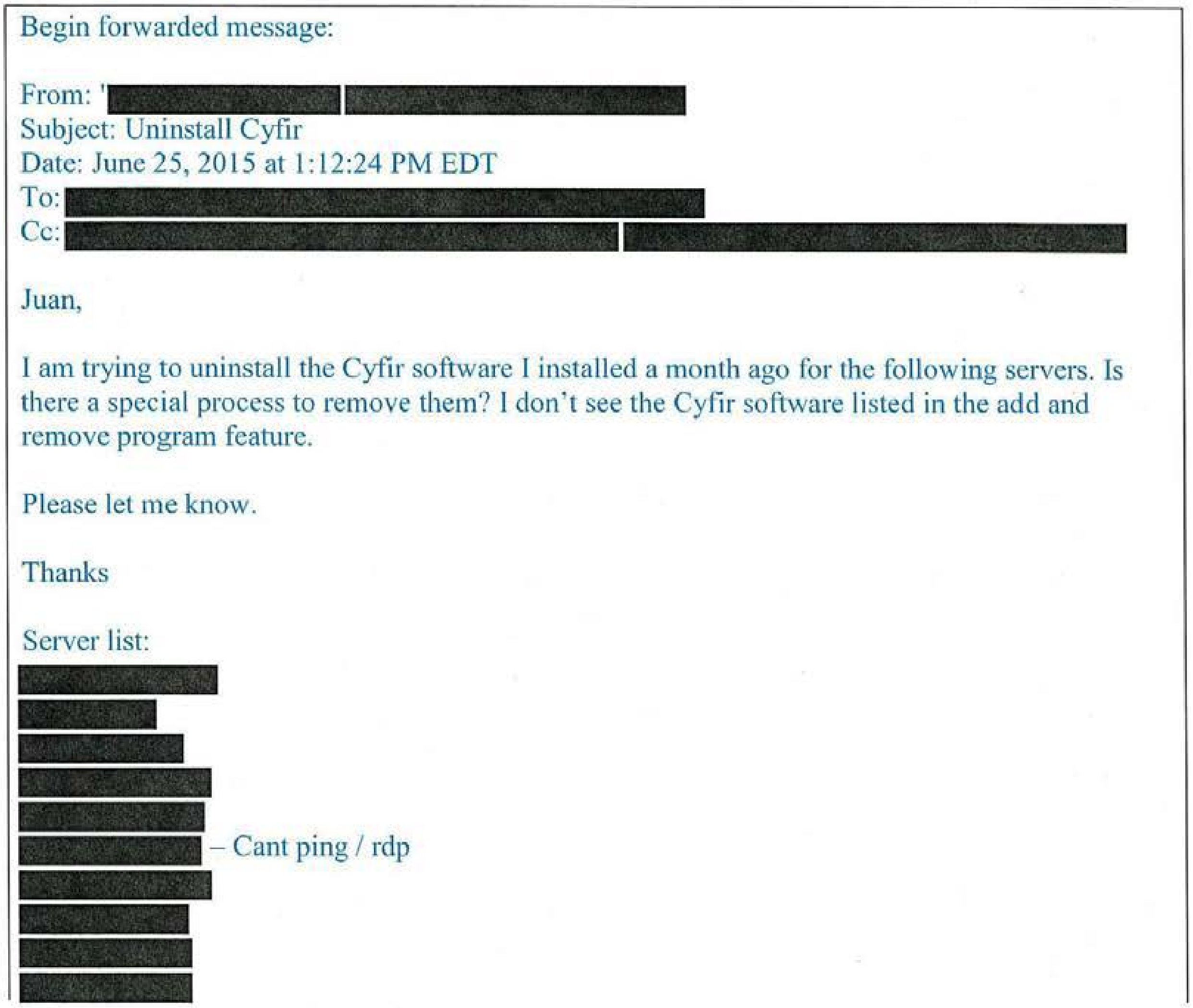
[716] Imperatis Weekly Report (May 18, 2015-May 22, 2015), Attach.6. at 000797 (Imperatis Production: Sept. 1, 2015).

[717] Email from [redacted] U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Off. of Pers. Mgmt. (June 2, 2015, 12:00 p.m.) at HOGR020316-000379 (OPM Production: Feb. 16, 2016).

[718] Wagner Tr. at 151.

[719] List of locations on which CyTech's CyFIR was tested at HOGR0724-000320- 321-UR (OPM Production Sept. 25, 2015). Initially, this document was provided with redactions that did not allow a cross reference with key

Documents show the CyFIR tool was deployed on the OPM system through June 2015, and that it was not fully uninstalled until August 2015. On June 25, 2015, an OPM IT official contacted Bonilla for instructions on how "to uninstall the Cyfir software . . . installed a month ago" from a list of more than forty servers, including several servers involved in the background investigation data breach.[720] This request for instructions to uninstall CyFIR occurred the day after former CIO Donna Seymour and Director Katherine Archuleta testified before the Committee about CyTech's involvement in the discovery of the data breach. Seymour and Archuleta testified that CyTech was not involved in the discovery of the data breach; and they did not disclose the involvement of Cylance, who, like CyTech, also did not have a contract in place when OPM's leadership was testifying before the Committee.[721]



Begin forwarded message:

From: '[redacted]
Subject: Uninstall Cyfir
Date: June 25, 2015 at 1:12:24 PM EDT
To: [redacted]
Cc: [redacted]

Juan,

I am trying to uninstall the Cyfir software I installed a month ago for the following servers. Is there a special process to remove them? I don't see the Cyfir software listed in the add and remove program feature.

Please let me know.

Thanks

Server list:

[redacted]

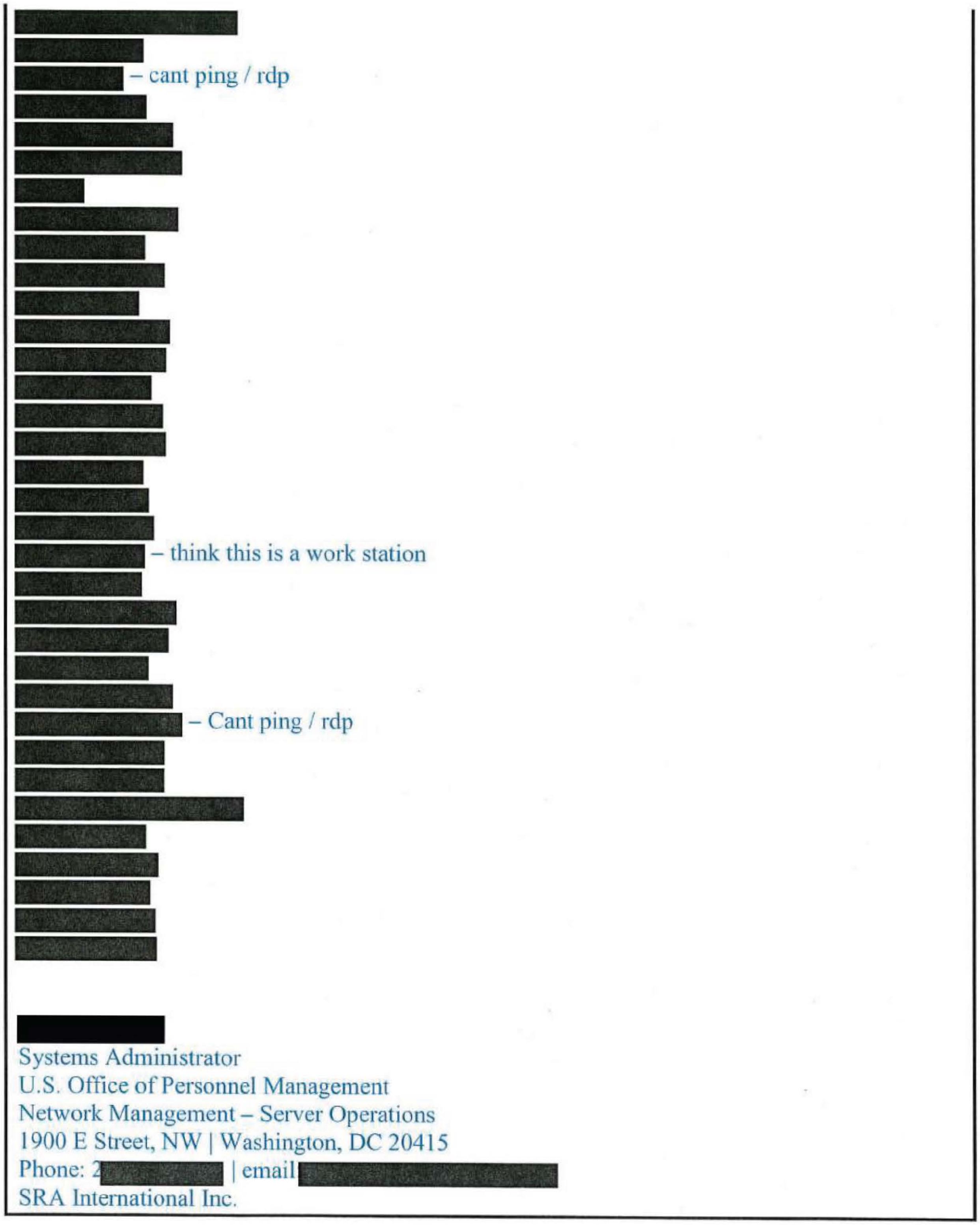
[redacted] – Cant ping / rdp

[redacted]

servers involved in the breach with where the CyFIR tool was deployed. In response to the Committee's February 3, 2016 subpoena OPM provided an unredacted version of this list on April 15, 2016.

[720] Email from [redacted], Contractor, U.S. Office of Pers. Mgmt., to Juan Bonilla, Senior Sec. Consultant, CyTech (June 25, 2015); Cotton Tr., Ex. 6; Wagner Tr. at 32-33.

[721] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Information Officer, Office of Personnel Management) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).



[redacted]

[redacted] – cant ping / rdp

[redacted]

[redacted] – think this is a work station

[redacted]

[redacted] – Cant ping / rdp

[redacted]

[redacted]

Systems Administrator
U.S. Office of Personnel Management
Network Management – Server Operations
1900 E Street, NW | Washington, DC 20415
Phone: 2[redacted] | email [redacted]
SRA International Inc.

Documents show OPM did not finish uninstalling CyFIR until August 2015. The Committee obtained internal agency emails that state the uninstall effort began on June 26, 2015